Overview Guide

SecureLogin 7.0 SP3

April, 2012

Novell

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This document provides to you an overview of the features, functionality, customizing, and administration of Novell SecureLogin.

Audience

This guide is intended for:

- Network administrators
- System administrators
- IT support staff
- End users

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to the Novell Feedback Web site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Documentation Updates

For the most recent version of the *Overview Guide*, visit the Novell Documentation Web site (http://www.novell.com/documentation/securelogin70).

Additional Documentation

For documentation on other Novell SecureLogin documentation, see the Novell SecureLogin Documentation Web site (http://www.novell.com/documentation/securelogin70).

The other documents available with this release of Novell SecureLogin are:

- *Getting Started*
  - *Novell SecureLogin Readme 7.0 SP3*
  - *Novell SecureLogin Overview Guide*
  - *Novell SecureLogin Quick Start Guide*

- *Installation*
  - *Novell SecureLogin Installation Guide*
- *Administration*
  - *Novell SecureLogin Administration Guide*
  - *Novell SecureLogin Application Definition Wizard Administration Guide*
  - *Novell SecureLogin Citrix and Terminal Services Guide*
  - *pcProx Guide*
- *End User*
  - *Novell SecureLogin User Guide*
- *Reference*
  - *Novell SecureLogin Application Definition Guide*

1 About Novell SecureLogin

In large enterprises and organizations, employees must interact with multiple applications and access sensitive information. Each application has its own authentication methods that require users to specify different usernames and passwords. This forces the users to maintain and manage different usernames and passwords to each of the numerous applications, which can be inconvenient and difficult.

To resolve these issues, a solution is needed to avoid the necessity of users remembering numerous passwords while simultaneously providing users access to the required sensitive data without compromising on security.

Novell SecureLogin is a single sign-on product that provides this kind of ease for password management.

Novell SecureLogin utilities and components are designed to enable single sign-on for Windows, Web, Java, and terminal emulator applications.

It supports both username and password authentication, and also multi-factor authentication such as smart card, token, or biometric authentication at the network and application levels.

Novell SecureLogin has the following features:

- Eliminates the requirement for users to remember multiple usernames and passwords beyond their initial login. It stores usernames and passwords and automatically specifies them for users when required. With this feature, users are no longer required to remember and manually provide their credentials to log in to an application.
- It quickly retrieves and specifies user credentials, which results in faster login.
- It helps reduce calls to the Help Desk about locked accounts and forgotten usernames and passwords.
- It makes use of multiple integrated security systems that provide authentication and single sign-on to networks and applications.

  It provides a single entry point to the corporate network and its user resources, which increases security and enhances compliance with corporate security policies.
- It stores and encrypts user credentials in the directory: eDirectory, Active Directory, or other LDAP-compliant directories, and optionally caches them in an encrypted format on the local workstation.

  With this level of encryption, an administrator with complete rights cannot view a user's credentials.

If required, an administrator can set a new password under some circumstances, such as disaster recovery, but cannot view the existing password.

- Client Login Extension 3.7 provides password recovery support for applications that are accessed through Novell SecureLogin 7.0 SP1. The password recovery support through Client Login Extension tool is also available for locked workstations and for workstations in which user operations are controlled by Desktop Automation Services (DAS).
- It employs two methods of fault tolerance:
  - It uses local encrypted caching to ensure that the network downtime does not affect the single sign-on performance. If the corporate network is down, caching enables application logins to continue uninterrupted.
  - It uses application definitions to cater to different login conditions and errors during the login.

It maintains single sign-on integrity for all mobile and remote users by locally encrypting the cache regardless of the network connectivity. If permitted, mobile users can update their single sign-on credentials when they are disconnected from the network and update the directory with these details when they attach later.

Because Novell SecureLogin is a directory-enabled product, users can:

- Log in from anywhere and get capabilities as if they were working from their own desks.
- Log in and log out quickly because they authenticate only to the directory, and not to Windows itself.
- Roam the enterprise and log in to different machines during the day.
- Work on a laptop in a disconnected mode because their login credentials are saved to a local, encrypted cache.
- Securely use a shared, kiosk-type workstation where many people log in temporarily for quick work, then log out.

Novell SecureLogin includes wizards, directory console plug-in, and tools which make it easy to centrally configure for use on the corporate network.

Includes management utilities that allows the administrators and end-users to view their single sign-on details and, if permitted enable single sign-on applications.

2 Novell SecureLogin Interface

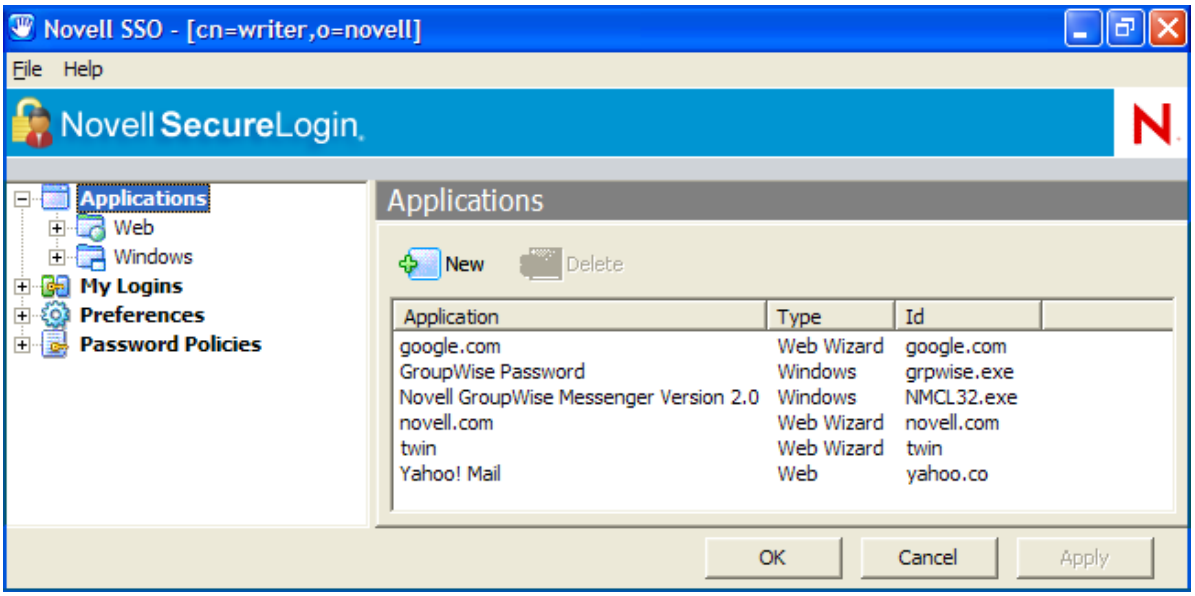
This section consists of the following sections:

2.1 Novell SecureLogin Client Utility

Novell SecureLogin Client Utility interface consists of a title bar, menu bar, panes, and properties tables.

When a folder in the navigation tree is selected, the related information is displayed in the right pane. To display the objects associated with the folders in the navigation tree, click the plus (+) symbol next to the icon to expand its contents.

Figure 2-1 *Novell SecureLogin Client Utility*



The navigation tree in the left pane contains the following:

- *Applications*
- *My Logins*
- *Preferences*
- *Password Policies*

Changes made by using Novell SecureLogin Client Utility on the local workstation apply only to the currently logged-in user's single sign-on and they override the settings made in the directory.

Novell SecureLogin Client Utility is used for:

- Providing the users with the capability to configure the Novell SecureLogin environment and view their credentials.
- Testing Novell SecureLogin configuration before mass deployment.
- Creating and modifying the application definitions for testing.
- The standalone mode.
- Troubleshooting.

For more information see, the *Novell SecureLogin Administration Guide*.

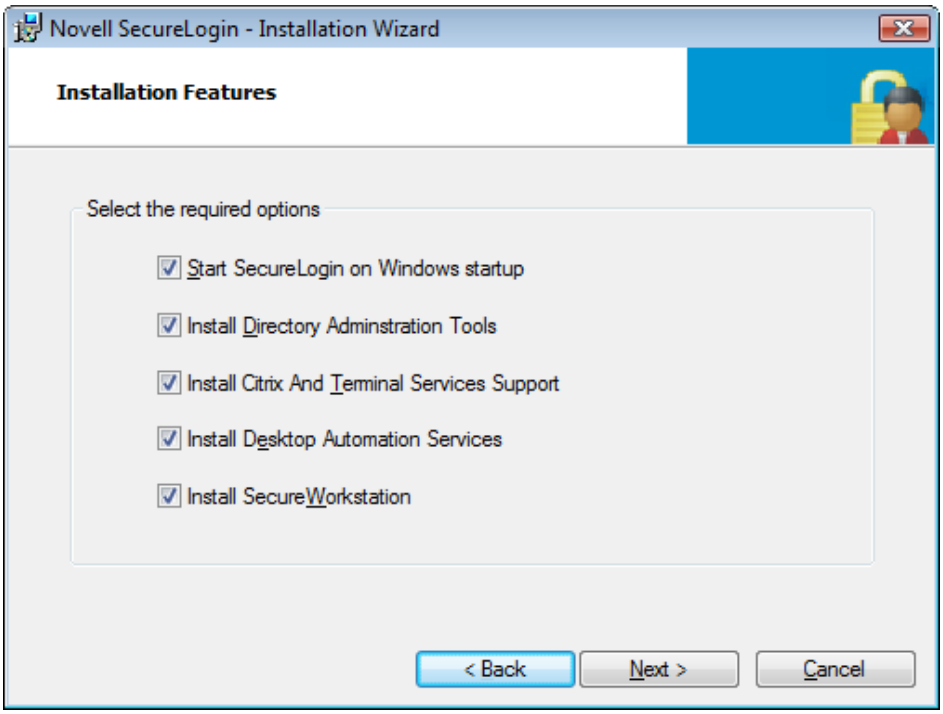
2.2 The Administrative Management Utilities

Novell SecureLogin consists of the Administrative Management utilities and plug-in for inclusion in Novell SecureLogin, which are used for administering Novell SecureLogin.

Through the Administrative Management utilities you can set up and administer Novell SecureLogin for a user.

IMPORTANT: The *Install Directory administration tools* option must be selected during Novell SecureLogin installation.

Figure 2-2 *Directory Administration Tools*



The utilities are:

- Section 2.2.1, "Novell iManager," on page 11
- Section 2.2.2, "SLManager," on page 13
- Section 2.2.3, "Microsoft Management Console Snap-In," on page 14

2.2.1 Novell iManager

Novell iManager is a state-of-the-art Web-based administration console that provides customized secure access to network administration utilities and content from any location in the world. With a global view of your network from one browser-based tool, you can proactively assess and respond to changing network demands.

IMPORTANT: Throughout this document, we refer to iManager as the Administrative management Utility to explain the various administration procedures.

The graphics also represent iManager set up.

Starting iManager

Accessing iManager varies based on the iManager version (server-based or workstation) and the platform on which iManager is running.

Accessing Server-Based iManager

1 In a supported Web browser, type the following in the Address (URL) field:

```
http://server_IP_address/nps/iManager.html
```

For example:
`http://127.0.0.1/nps/iManager.html`

You might be redirected to an HTTPS secure page

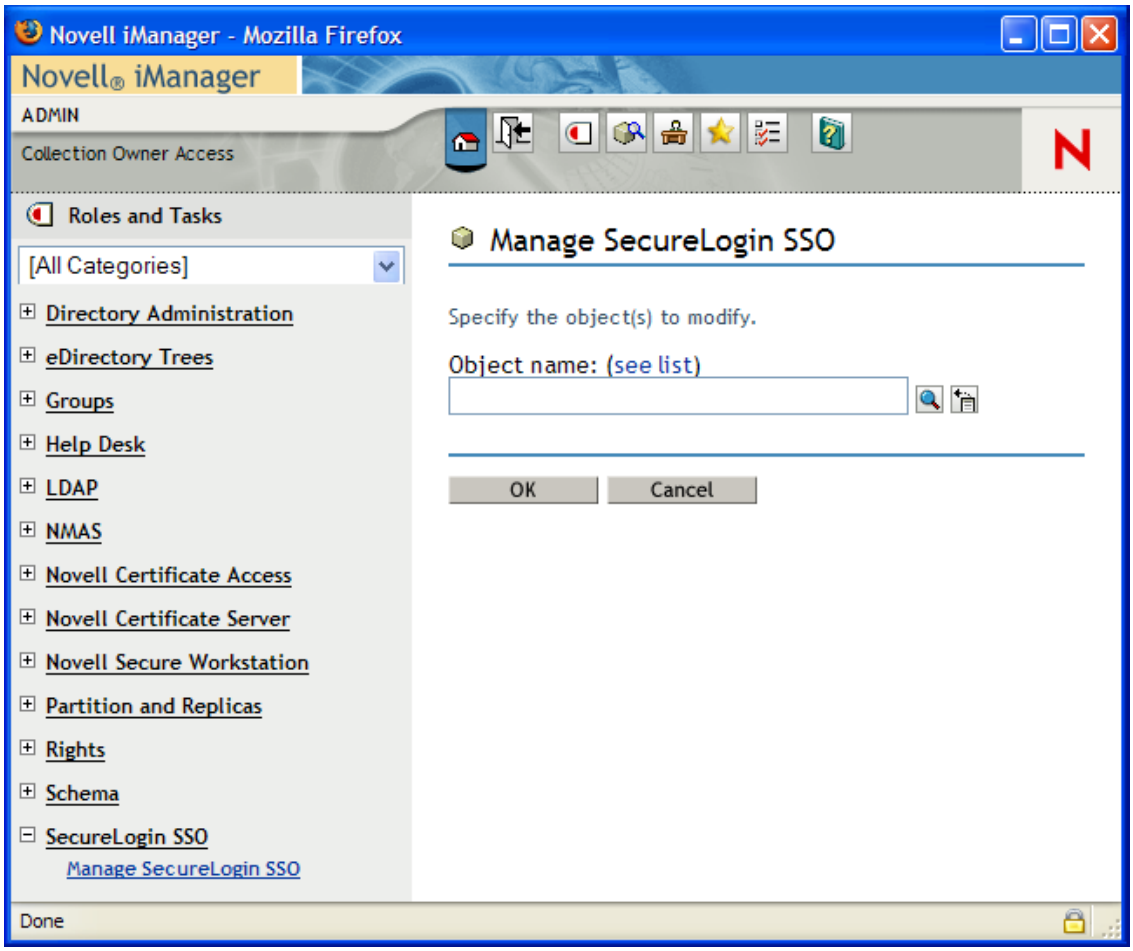
IMPORTANT: The URL is case sensitive.

---

2 Log in using your username, password, and eDirectory tree name.

You can substitute the IP address of an eDirectory server for the tree name.

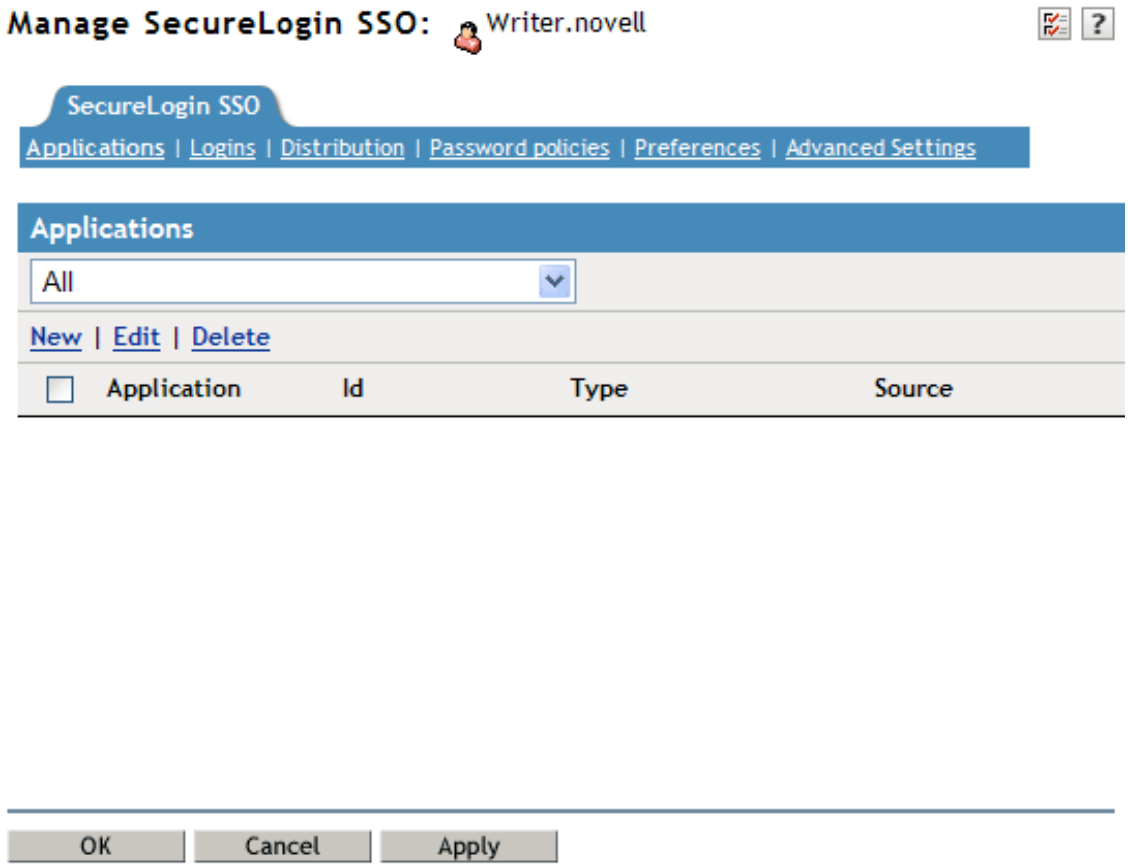
To have full access to all Novell iManager features, you must log in as a user with administrator-equivalent rights to the tree.



For details on accessing iManager, go to the Novell Documentation Web site for iManager (http://www.novell.com/documentation/imanager27/imanager_install_27/?page=/documentation/imanager27/imanager_install_27/data/alw39eb.html)

For accessing and using SecureLogin Manager refer, "Starting iManager" on page 11.

3 Click *OK*. The SecureLogin SSO page with the single sign-on options is displayed.



Accessing iManager on a Workstation

1 Browse to the iManager set up on your workstation.

2 Execute `imanager\bin\iManager.bat`.

3 Log in by using your username, password, and tree name.

The navigation tree in the top consists of the following options:

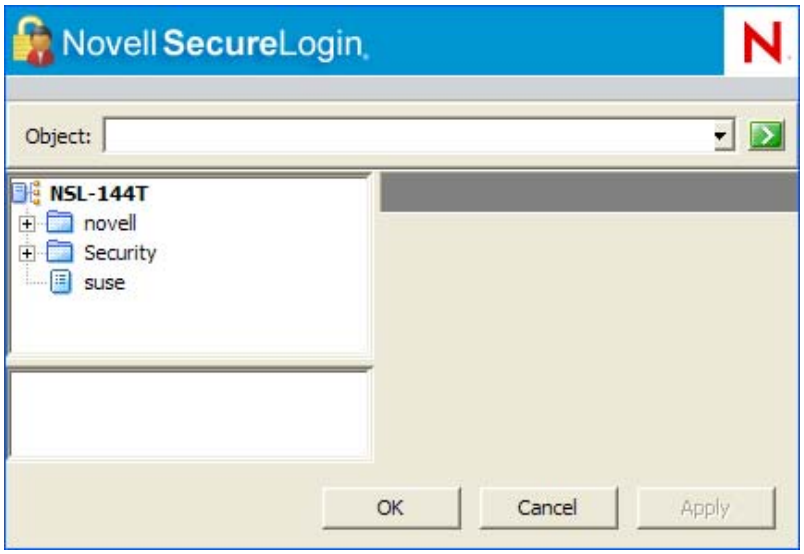
- *Applications*
- *Logins*
- *Distribution*
- *Password Policies*
- *Preferences*
- *Advanced Settings*

NOTE: The same options are available in SecureLogin Manager too.

2.2.2 SLManager

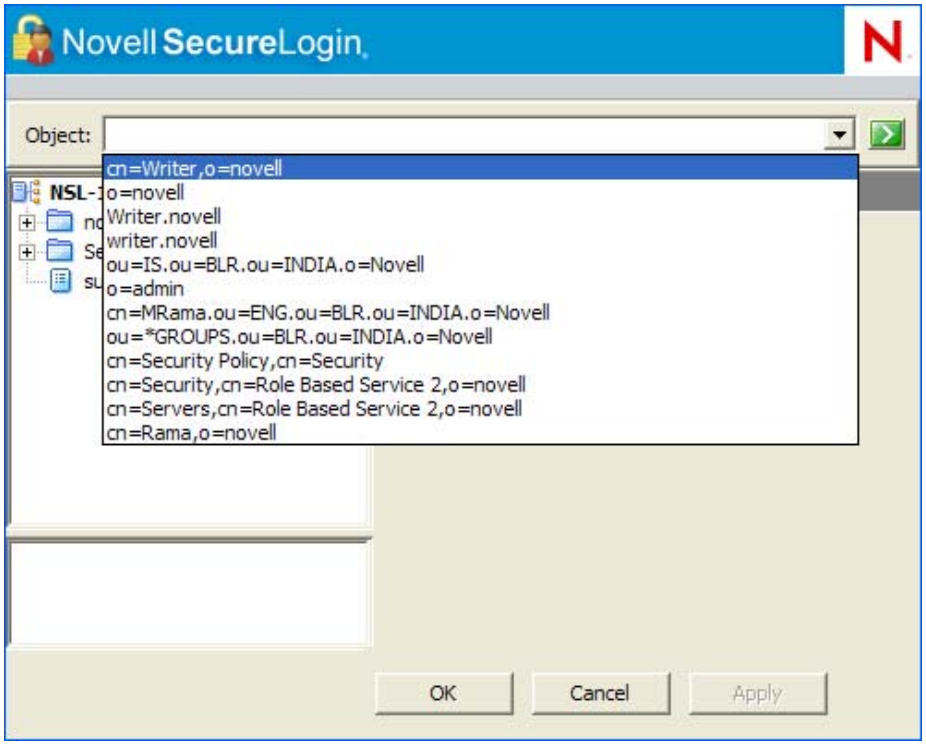
1 Click *Start* > *Programs* > *Novell SecureLogin* > *SecureLogin Manager*.

The SecureLogin Manager is displayed.



2 From the *Object* drop-down list, select the object or specify the full distinguished name (DN) of the user object, container, or the organizational unit for administration.

Alternatively, use the  icon to navigate to the appropriate object.



3 Press Enter to submit the entry specified in the object field.

Clicking *OK* closes the dialog box and cancels the specified entry.

2.2.3 Microsoft Management Console Snap-In

Use the Microsoft Management Console (MMC) snap-in for Active Directory deployments.

Starting MMC

1 On the Windows *Start* menu, select *Programs* > *Administrative Tools* > *Active Directory Users and Computers*. The Microsoft Management Console is displayed.

2.3 Novell SecureLogin Icon

Novell SecureLogin icon appears on the workstation's notification area (system tray) and provides quick access to common functions in the management utilities and wizards.

Table 2-1 *Novell SecureLogin Icon Status*

If	Then
Novell SecureLogin is active.	Novell SecureLogin icon appears on the notification area as .
Novell SecureLogin is inactive.	Novell SecureLogin icon appears on the notification area as . **NOTE:** In this case, Novell SecureLogin does not perform single sign-on functions such as decrypting and passing credentials to applications.

Following are the options that are available by right-clicking Novell SecureLogin icon on the notification area.

Table 2-2 *Novell SecureLogin Icon Menu Options*

Option	Function
Add Applications	Launches the Add Application Wizard.
Manage Logins	Launches Novell SecureLogin Client Utility.
New Login	Launches the Add New Login Wizard.
Advanced	Has some advanced Novell SecureLogin management options. See Table 2-3 on page 16.
Active	Displays a check (✓) mark when Novell SecureLogin is active on the workstation.
About	Displays information about Novell SecureLogin and your system.
Log Off User	Allows you to shut down all programs, including Novell SecureLogin, and log out the user from the workstation.
Close	Closes Novell SecureLogin on the workstation.

Following are the options available on the *Advanced* menu:

Table 2-3 *Novell SecureLogin Advanced Menu Options*

Option	Function
Change Preferences	Launches Novell SecureLogin Client Utility with the *Preferences* properties table displayed.
Change Passphrase	Displays the *Passphrase* dialog box. It enables users to change their passphrase answer.
Refresh Cache	Manually executes the synchronization of data between the local cache and directory data.
Backup User Information	Enables local workstation settings. This includes credentials that can be saved as an XML file.
Restore User Information	Enables the XML file that is backed up to be restored in the local workstation single sign-on cache.
Work Offline / *Work Online*	Toggles between offline and online network access. Displays whether the user is connected to the network or not. **NOTE:** This is not displayed in standalone mode.

2.4 Application Types and Descriptions

The following table describes the application type icons as available in SecureLogin Manager:

Table 2-4 *Application Types and Description*

Icon	Application Type	Description
	Generic	The name of the application executable.
	Java	◆ The Web page URL containing the JavaScript login, for example, `http:/javaboutique.internet.com/KiserPassword`. ◆ Class name of the application (if it is a stand-alone Java application).
	Startup	This must be configured in the application definition editor. For more information, see the *Novell SecureLogin Application Definition Guide*.
	Terminal Emulator	The name of the emulator. For example, `PLAY3270.A3D`.
	Web	All or part of the URL of the Web page or an application. The name can apply to an entire Web site or a specific Web page. For example, the domain name `www.novell.com` activates Novell SecureLogin application definition on any page on the Novell Web site. Alternatively, `www.novell.com/` activates the application definition solely on the specified Web page.
	Windows	The name of the application executable, for example, `notepad.exe`.

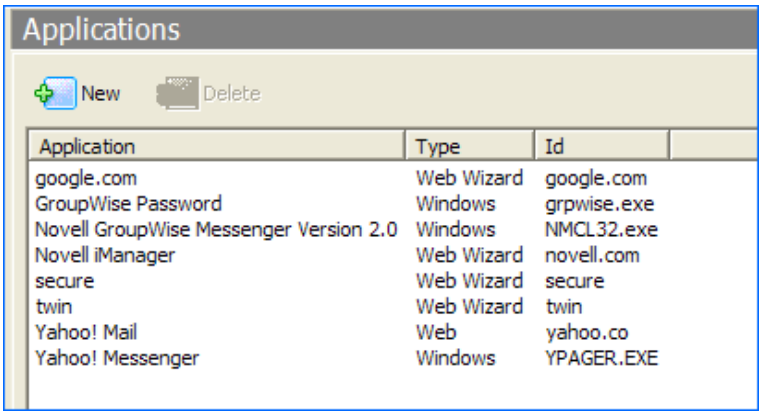
The following table describes the application details icons as available in SecureLogin Manager:

Table 2-5 *Application Details*

Icon	Description
	A red triangle in the lower right corner of an application icon denotes a corporate application definition. A corporate application definition is the one that is inherited from a higher-level object, for example, an organizational unit.
	An application icon without the red triangle in the lower corner is an application definition or a predefined application that is not inherited from a higher-level object.

2.5 The Applications Pane

Figure 2-3 *The Applications Pane in SecureLogin Manager*



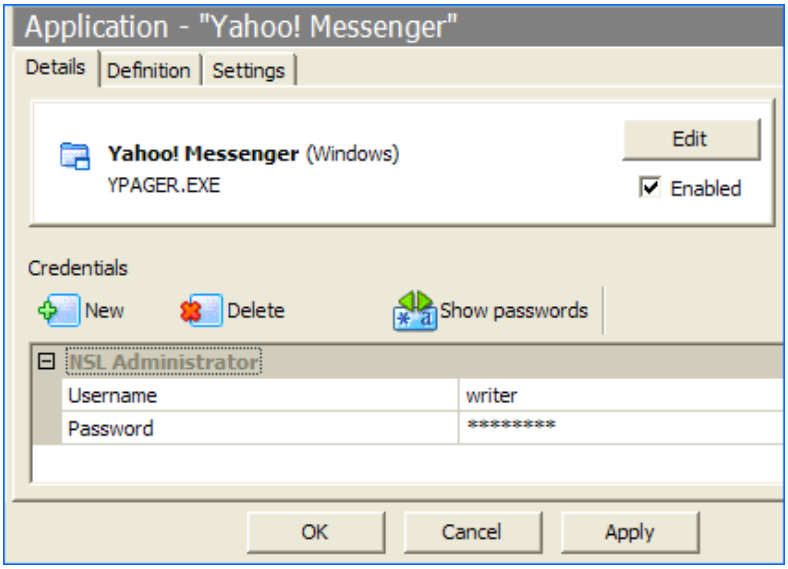
From the applications pane, users can create and modify Novell SecureLogin application definitions that enable the single sign-on. For details, see the *Novell SecureLogin Application Definition Guide*.

To display a specific application, double-click an application in the navigation tree or in the Application pane. The Application pane for that specific application is displayed. It contains three tabs:

- Section 2.5.1, “The Details Tab,” on page 18
- Section 2.5.2, “The Definition Tab,” on page 18
- Section 2.5.3, “The Settings Tab,” on page 18

2.5.1 The Details Tab

Figure 2-4 *The Details Tab in SecureLogin Manager*



The *Details* tab contains:

- The Application description that uniquely identifies the application definition or the predefined application along with the type of the application. The application definition or the predefined application definition is either the name given by Novell SecureLogin or the name specified by the user.
- The Application name.
- The credentials (login) linked to the application and tools to create, edit, and delete these credentials.

2.5.2 The Definition Tab

The *Definition* tab contains the application definition. An application definition directs how Novell SecureLogin responds to various screens (dialog boxes) returned by the application. The details displayed are either the application definition created by Novell SecureLogin when the predefined application or the application definition was added, or when the application definition was manually created by the user.

NOTE: Predefined Web applications such as eBay and Hotmail under the *Type* option are titled *Web* and not *Advanced Web*. There is no difference between a Web application definition and an Advanced Web application definition.

2.5.3 The Settings Tab

The *Settings* tab contains the advanced options for the predefined application or the application definition.

The following table describes the settings for Terminal Emulator, Windows, Startup, Java, and Generic Applications:

Table 2-6 *Settings for the Windows Applications*

Item	Description
Prompt for device reauthentication for this application	If *Yes* is selected, users are prompted for device reauthentication for the application.
Reauthentication Method	Allows the user to reauthenticate an application against an AA device where Novell SecureLogin is used in conjunction with NMAS infrastructure.

The following table describes the settings for Web applications:

Table 2-7 *Settings for Web Applications*

Item	Description
Allow web page to load while Application Definition is running (Web applications only)	This applies to Microsoft Internet Explorer and the application definitions created for Web pages and JavaScript logins that are executed in a Web page. By default, this option is set to *No*. This suspends the completion of any other Internet Explorer tasks until the login is completed. If this option is set to *Yes*, then the Internet Explorer continues to function while Novell SecureLogin is executing the login.
Password field must exist on Internet Explorer page for Application Definition to run (Web applications only)	This applies to the Microsoft Internet Explorer and application definitions created for the Web pages and JavaScripts within the Web pages. If *Yes* is selected, it ensures that Novell SecureLogin does not execute the automated login on pages without the password field. If *No* is selected, the Web application returns errors on pages without the password fields that you need to handle with Novell SecureLogin. For example, the *Change Successful* message.

2.6 The Logins Pane

The *My Logins* pane in Novell SecureLogin Client Utility manages the logins that applications require to log in, along with their associated credentials, including:

- Username
- User ID
- Login ID
- Password
- PINs
- Domain
- Database names
- Server IP address

Through the Logins pane, the user can:

- Link the logins manually, including the host IP addresses to the applications.

- Configure the credential sets at the Group policy, organizational unit, container, and the user object level.
- Enable the group of users to be configured with seamless login access to an application with one account or by logging in with the username and password.

2.7 The Preferences Properties Table

The *Preferences* properties table provides tools to configure the parameters of the user's Novell SecureLogin environment, including applications permitted to be enabled for single sign-on and access to Novell SecureLogin management and administration tools.

The following table provides the options for Novell SecureLogin Client Utility, the SecureLogin Manager, and iManager. If the option is available only in one of the management utilities, this is mentioned in the Description column in the following Preferences tables.

2.7.1 Configuring Preferences Introduced In Novell SecureLogin Version 6

Prior to configuring preferences, administrators should refer to the *Novell SecureLogin Administration Guide* for important information regarding Novell SecureLogin functionality using different datastore versions, particularly in mixed or staged deployments.

Novell SecureLogin version 6 introduced a range of new security features and preferences, including the storage of single sign-on credentials on the user's smart card, encryption of the data store using Public Key Infrastructure (PKI)-based credentials and support for the Advanced Encryption Standard (AES) encryption algorithm. These new preferences required changes to Novell SecureLogin 6.0 datastore format to support them.

Viewing and modifying application definitions

Novell SecureLogin 6.0 and earlier had a single preference titled *Allow users to view and modify application definitions* that is superseded by two separate preferences for viewing and modifying application definitions.

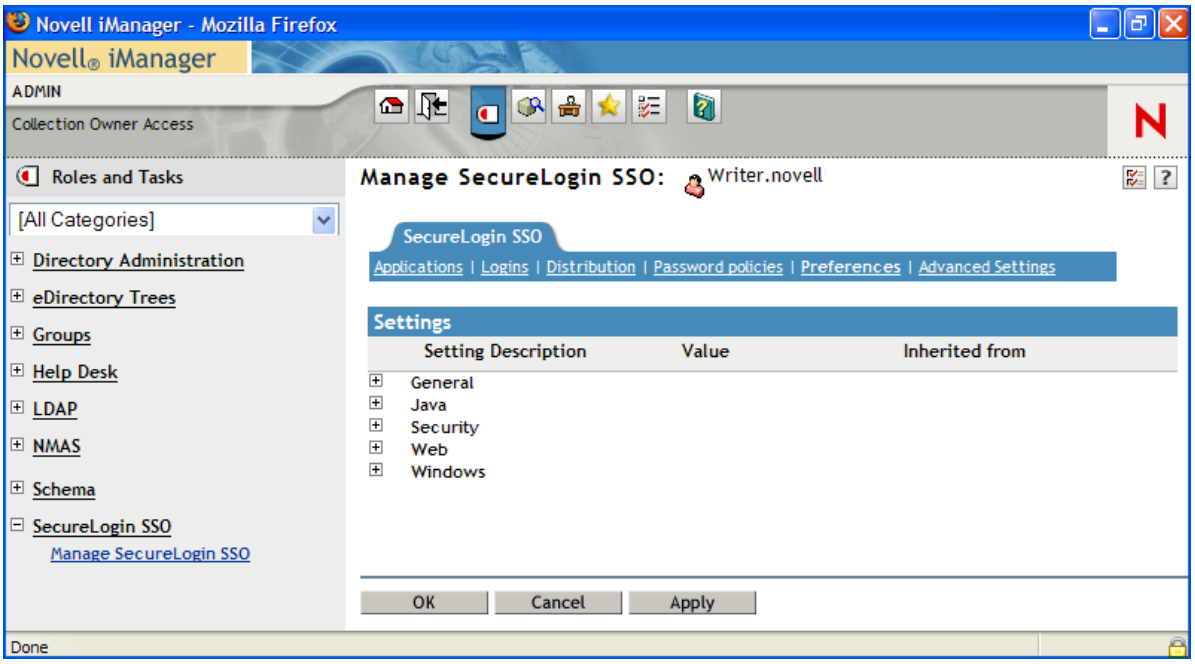
When upgrading from earlier versions of Novell SecureLogin to version 6.1 or later using legacy directory data, old *Allow users to view and modify application definitions* was set to *No*, then the new *Allow application definition to be modified by users* preferences for the current version will be disabled (grayed out).

You must reset *Allow application definition to be viewed by users* to *Yes* before users can modify application definitions.

The *Preferences* are displayed on the right pane when *Preferences* is clicked in the Management utility.

Click the plus (+) symbol next to the names of the preferences to expand the preference options.

Figure 2-5 *The Preferences*



In previous versions of Novell SecureLogin, the application definition preference was a single preference called *Allow users to view and modify application definitions*. This is now split into two preferences:

- *Allow application definition to be modified by users*
- *Allow application definition to be viewed by users*

When you upgrade from a previous version of Novell SecureLogin to Novell SecureLogin 7.0, if you are using the legacy directory data (that is, data from Novell SecureLogin 6.0 or 3.5) and if the *Allow users to view and modify application definition to be modified by users* option was set to *No*, then the new *Allow application definition to be modified by users* for Novell SecureLogin 7.0 is disabled and dimmed.

Administrators must reset the *Allow application definition to be viewed by users* option to *Yes* before users can modify the application definitions.

The Preferences has the following categories:

- Table 2-8, “The General Preferences Properties Table,” on page 22
- Table 2-9, “The Security Preferences Properties Table,” on page 32
- Table 2-10, “The Java Preferences Properties Table,” on page 36
- Table 2-11, “The Web Preferences Properties Table,” on page 37
- Table 2-12, “The Windows Preferences Properties Table,” on page 38

User or the administrators can change the value of the Preferences in the Administrative Management utility or Novell SecureLogin Client Utility unless otherwise specified.

The administrators can restrict the user’s access to this table through the centrally controlled administrative preferences.

NOTE: The *Security* option is not available in Novell SecureLogin Client Utility.

Table 2-8 *The General Preferences Properties Table*

Preference	Possible Values	Description	Default Value
Allow "Close" option via system tray	*Yes*/*No*/*Default*	This preference controls whether users can access the *Close* option from Novell SecureLogin icon on the notification area (system tray). If the option is set to *No*, the *Close* option is shown as disabled in the Novell SecureLogin notification area (system tray) icon. If this option is set to Yes or *Default*, the *Close* option is displayed and accessible in the Novell SecureLogin notification area (system tray) icon. **NOTE:** This preference requires Novell SecureLogin 6.0 datastore if the value is changed. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Allow "Refresh Cache" option via system tray	*Yes*/*No*/*Default*	This preference controls whether users can refresh cache using the *Advanced > Refresh Cache* option from the Novell SecureLogin icon on the notification area (system tray). If this option is set to *Yes*, the *Refresh Cache* option is displayed and accessible in the notification area (system tray) icon. If this option is set to *No* or *Default*, the *Refresh Cache* option is not displayed in the notification area (system tray) icon. **NOTE:** This preference requires Novell SecureLogin 6.0 datastore if the value is changed. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *No*.
Allow "Log Off" option via system tray	*Yes*/*No*/*Default*	This preference controls if users can log out from a session using *Log Off User* option from the Novell SecureLogin icon on the notification area (system tray). If this option is set to *No*, the *Log Off User* option is not displayed and accessible in the Novell SecureLogin notification area (system tray) icon. If this option is set to *Yes* or *Default*, the *Log Off User* option is displayed and accessible in the Novell SecureLogin notification area (system tray) icon. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Preference	Possible Values	Description	Default Value
Allow "Work Offline" option via system tray	*Yes*/*No*/*Default*	This preference controls whether users can work in offline cache mode using the *Advanced* > *Work Offline* option. If this option is set to *Yes* or *Default*, the *Work Offline* option is displayed in the notification area (system tray) icon. If this option is set to *No*, the *Work Offline* option is not displayed in the notification area (system tray) icon. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Allow application definition to be modified by users	*Yes*/*No*/*Default*	This preference controls whether users can modify application definitions using the *Definitions* tabs in the Applications pane of the Novell SecureLogin Client Utility. If this option is set to *Yes* or *Default*, the end user can view and modify their application definitions. If this option is set to *No*, the end user cannot change their application definitions. **NOTE:** If the Allow application definition to be viewed by users is set to No, then this option is cannot be edited. Disabling this preference does not disable the users from creating new applications through the wizards. This preference requires Novell SecureLogin 6.0 datastore if the value is changed. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default option is *Yes*.
Allow application definition to be viewed by users	*Yes*/*No*/*Default*	This preference controls whether users can view application definitions using the *Definitions* tabs in the Applications pane of the Novell SecureLogin Client Utility. If this option is set to *Yes* or *Default*, users can view the application definition. If this option is set to *No*, users cannot view the application definition. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Preference	Possible Values	Description	Default Value
Allow credentials to be deleted by users through the GUI	*Yes*/*No*/*Default*	This preference controls whether users can delete their credentials using the Novell SecureLogin Client Utility available from Manage Logins from the Novell SecureLogin icon in the notification area (system tray). **NOTE:** If Allow credentials to be modified by users through the GUI is set to *No*, then this option is automatically set to *No* and not editable. This preference requires Novell SecureLogin 6.0 datastore if the value is changed. If this option is set to *Yes* or *Default*, users can delete their credentials through the GUI. If this option is set to *No*, users cannot delete their credentials. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Allow credentials to be modified by users through the GUI	*Yes*/*No*/*Default*	This preference controls whether users can modify their credentials using the Novell SecureLogin Client Utility available from Manage Logins from the Novell SecureLogin icon in the notification area (system tray). If this option is set to *Yes* or *Default*, users can modify their credentials through the GUI. If this option is set to *No*, users cannot modify their credentials through the GUI. They can only view the credentials. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Preference	Possible Values	Description	Default Value
Allow users to (de) activate SSO via system tray	*Yes*/*No*/*Default*	This preference controls whether users can activate or deactivate SecureLogin through the SecureLogin icon in the notification area (system tray). If this option is set to *Yes* or *Default*, users can switch between active and inactive modes of Novell SecureLogin. If this option is set to *No*, users cannot switch between active and inactive modes. ◆ If SecureLogin status was active when this preference was applied, it remains as active and the user cannot de-activate SecureLogin. ◆ If SecureLogin status was inactive when this preference was applied, it remains as inactive and the user cannot change SecureLogin status to *Active*. This preference requires Novell SecureLogin 6.0 datastore if the value is changed. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Allow users to backup/restore	*Yes*/*No*/*Default*	This preference controls whether users can backup and restore their information from the *Advanced* menu of the SecureLogin icon on the notification area (system tray). If this option is set to *Yes* or *Default*, users can back up and restore their single sign-on information. If this option is set to *No*, users cannot back up and restore their single sign-on configuration. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Preference	Possible Values	Description	Default Value
Allow users to change passphrase	*Yes*/*No*/*Default*	This preference controls whether users can change their passphrase question and answer. The *Change Passphrase* option is available from the *Advanced* menu of the Novell SecureLogin icon on the notification area (system tray). If this option is set to *Yes* or *Default*, users can change their passphrase through the notification area (system tray) icon. If this option is set to *No*, users cannot change their passphrase through the notification area (system tray) icon. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Allow users to modify names of Applications and Logins	*Yes*/*No*/*Default*	This preference controls whether users can edit the names of their Application login credentials using the *Details* tab > *Edit* function in the Novell SecureLogin Client Utility. If this option is set to *Yes* or *Default*, the user can edit the names of their credentials (either by right-clicking on the credential and selecting Rename, or by a slow double-click on the credential name). If this option is set to *No*, the use cannot edit the names of the credentials. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *No*.
Allow users to view and change Preferences	*Yes*/*No*/*Default*	This preference controls whether users can view and update their preferences. If this option is set to *Yes* or *Default*, users can view and change their preferences. If this option is set to *No*, users cannot view and change their preferences. **NOTE:** Create a separate ou for administrators to ensure that they are not adversely affected by the general user configuration preferences at the ou level. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Preference	Possible Values	Description	Default Value
Allow users to view and modify API preferences	*Yes*/*No*/*Default*	This preference controls whether users can view and modify API options using the Preferences pane of the Novell SecureLogin Client Utility. The API preference defines the following options for users to: ◆ Enter an API license key(s). ◆ Provide API access. If this option is set to *Yes* or *Default* users can view and modify the API preference. If this option is set to *No*, users cannot view and modify the API preference. **NOTE:** This preference affects what is displayed in the Novell SecureLogin Client Utility using Change Preferences from the Advanced menu. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Allow users to view passwords	*Yes*/*Yes, per application*/*No*/*Default*	This preference controls whether users can view their passwords using *Show Passwords* in the *Application* pane > *Details* of the Novell SecureLogin Client Utility. If this option is set to *Yes* or *Default*, users can view their passwords. If this option is set to *No*, users cannot view their passwords. **NOTE:** Allowing users to view their passwords gives them an opportunity to view and record passwords if they need to reset the Novell SecureLogin configuration. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Change the cache refresh interval (in minutes)	*5*	This preference defines the time in minutes the synchronization of user data and directory on the local workstation. This preference is available in both the Novell SecureLogin Client Utility and the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is set to *5* minutes.

Preference	Possible Values	Description	Default Value
Detect incorrect passwords	*Yes*/*No*/*Default*	Predefined applications generally include commands to respond to incorrect password dialogs. This preference enables SecureLogin to respond to incorrect passwords for web applications. If this option is set to *Yes* or *Default*, incorrect passwords for Web applications are detected. If this option is set to *No*, incorrect passwords for Web applications are not detected. This preference is available in both the Novell SecureLogin Client Utility and the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Disable single sign-on	*Yes*/*No*/*Default*	This preference controls the users access to running Novell SecureLogin. If this option is set to *Yes*, access to Novell SecureLogin is disabled and it will not start when run either automatically at startup or when run manually. If this option is set to *No* or *Default*, access to Novell SecureLogin is enabled and will start normally. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *No*.
Display splash screen on startup	*Yes*/*No*/*Default*	This preference controls the display of the Novell SecureLogin splash screen during startup. If this option is set to *Yes* or *Default*, the splash screen appears when Novell SecureLogin startsup. If this option is set to *No*, the splash screen is hidden and users cannot see the splash screen when Novell SecureLogin startsup. **NOTE:** This preference requires Novell SecureLogin 6.0 datastore if the value is changed. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Preference	Possible Values	Description	Default Value
Display the system tray icon	*Yes*/*No*/*Default*	This preference controls the display of Novell SecureLogin icon in the notification area (system tray). If this option is set to *Yes* or *Default*, the Novell SecureLogin icon appears on the notification area (system tray). If this option is set to *No*, the Novell SecureLogin icon does not appear on the notification area (system tray). **NOTE:** When the Novell SecureLogin icon is visible, users can double-click the icon on the notification area (system tray) to launch the Novell SecureLogin Client Utility. When the Novell SecureLogin is not visible, users can start the Novell SecureLogin Client Utility through *Start* > *Programs* > *Novell SecureLogin* > *Novell SecureLogin* This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Enable cache file	*Yes*/*No*/*Default*	This preference controls creating and updating of a SecureLogin cache file on the local workstation. The cache file stores all user configuration data; local and inherited. Set this option to *Yes* or *Default*, the cache file is saved on the local workstation in the directory that was specified during install. Users with roaming profiles should always have this setting as *Yes*. Set this option to *No* if you cannot store cache files locally or if this causes conflicts with your organizational security policy. This preference is available in both the Novell SecureLogin Client Utility and the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Preference	Possible Values	Description	Default Value
Enable logging to Windows Event log	*Yes*/*No*/*Default*	This preference controls sending the log events to Windows Event Log. This includes the entire user configuration, both local and inherited. If set to *Yes* or *Default*, log events are sent automatically to Windows Event Log. If set to *No*, the log events are not sent to Windows Event Log. Only the following events are logged: ◆ SSO client started ◆ SSO client exited ◆ SSO client activated by user ◆ SSO client deactivated by user ◆ Password provided to an application by a script ◆ Password changed by the user in response to a change password command ◆ Password changed automatically in response to a change password command. **NOTE:** This preference requires Novell SecureLogin 6.0 datastore if the value is changed. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Enable the New Login Wizard on the system tray icon	*Yes*/*No*/*Default*	This preference controls whether users can create multiple logins on the same application using the *New Login > Add New Login* option from the Novell SecureLogin icon on the notification area (system tray). If this option is set to *Yes* or *Default*, the New Login menu option is enabled and users can create multiple logins. If this option is set to *No*, New Login menu option is disabled and users cannot create multiple logins. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Preference	Possible Values	Description	Default Value
Enforce passphrase use	*Yes*/*No*/*Default*	This preference forces users to set up a passphrase question and answer when Novell SecureLogin is launched by a user for the first time. If this option is set to *Yes*, users must complete setting up their passphrase before they proceed with any other activity on the workstation. If this option is set to *No* or *Default*, users can postpone setting up the passphrase. If the users clicks *Cancel* or closes the dialog, then SecureLogin does not start. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *No*.
Enter API license key(s)	Specify API license key(s)	Specify the API license key(s) provided by Novell SecureLogin to activate the API functionality for an application. You can add more than one API license key. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	Specify the API license key
Password protect the system tray icon	*Yes*/*No*/*Default*	This preference restricts the users from accessing the Novell SecureLogin icon menu option (from the notification area (system tray) without their network login password. If this option is set to *Yes*, the Novell SecureLogin icon on the notification area (system tray) is password protected. If this option is set to *No* or *Default*, the Novell SecureLogin icon on the notification area (system tray) is not password protected. This preference is available in both the Novell SecureLogin Client Utility and the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *No*.
Provide API Access	*Yes*/*No*/*Default*	This preference controls the API functionality use. If this option is set to *Yes*, the API access is enabled. If this option is set to *No* or *Default*, the API access is disabled. This preference is available in both the Novell SecureLogin Client Utility and the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *No*.

Preference	Possible Values	Description	Default Value
Stop walking here	*Yes*/*No*/*Default*	This preference controls the inheritance of settings from higher level containers or organizational units. If this option is set to Yes, the inheritance of settings from higher level containers or organizational units is disabled. Set the option to *Yes* during phased upgrades when higher levels might have a different version of Novell SecureLogin implemented. If this option is set to *No* or *Default*, the inheritance of settings from higher level containers or organizational units is enabled. This preference does not apply when Novell SecureLogin is installed in eDirectory environment. The Corporate redirection functionality; that is, the inheritance settings from higher level container or organizational units is bypassed in an eDirectory environment. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *No*.
Wizard mode	*Administrator*/ *User*/*Disabled*	This preference controls that access to the application definition wizard. If this option is set to *Administrator*, it gives users' complete access to the application definition wizard. Users can create their own application definitions. If this option is set to *User*, users are only allowed to create new login credential sets for new applications using the auto-detection settings. If this option is set to *Disabled*, the application definition wizard is not launched. **NOTE:** This preference requires Novell SecureLogin 6.0 datastore if the value is changed. This preference is available through the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Administrator*.

Table 2-9 *The Security Preferences Properties Table*

Preference	Possible Values	Description	Default Value
Certificate selection criteria	Specify text to identify your certificate	This preference allows you to specify a text to uniquely identify a certificate (within searchable field only).	Not applicable
Current certificate	No certificate selected	This preference allows you to select a certificate other than the default certificate.	Not applicable

Preference	Possible Values	Description	Default Value
Enable passphrase security system	*Yes*/*No*/*Hidden*	This passphrase is an additional mechanism for unlocking a user's single sign-on data if the primary key (network password, smartcard, or PIN) used to encrypt the single sign-on data is lost or forgotten. It also prevents unauthorized access to a user's single sign-on data in the event their primary key is deliberately changed by a third party. In this case even if the unauthorized person is able to bypass a user's primary key, he or she must answer the passphrase answer to access the user's single sign-on data. If this option is set to *Yes* or *Default*, the correct passphrase answer is prompted in situations where the user cannot provide the primary key (network password, smart card, or PIN). If the correct passphrase answer is not provided, SSO data will not be available to the user. If you change the preference from *Hidden* to *Yes* after the user has set up a passphrase, users must answer the passphrase questions to use Novell SecureLogin. Typically, users not prompted to create a passphrase after the first login. If this option is set to *Hidden*, the user is not requested to answer a passphrase question. It is automatically generated by SecureLogin according to the user's parameters. This process is then automatically used in the configuration where a passphrase is required. If this option is set to *No*, the passphrase system is not enabled and cannot be used. If the primary key is lost or forgotten, users' single sign-on data cannot be accessed. You can set this preference to *No* if the preference for *Use smart card to encrypt SSO data* is also set to *PKI Credentials*. **NOTE:** The Enable passphrase security system preference is supported only with the datastore version 6.0. The Disable passphrase security system preference applicable for datastore version 3.5 is removed and is no longer supported. If you are using this preference with datastore version 3.5, you must upgrade the datastore version 6.0 to use the Enable passphrase security system preference.	

Preference	Possible Values	Description	Default Value
Lost card scenario	*Allow passphrase*/ *Require smart card*	This preference determines how Novell SecureLogin handles a user forgetting, losing or damaging his or her smart card. The *Lost card* option can only be used if the *Enable passphrase security system* option is set to *Yes* or *Hidden* and Use smart card to encrypt single sign-on data is set to one of the smart card values. If this option is set to *Allow passphrase* or *Default*, the passphrase functions as a secondary key. If the smart card is not available, the passphrase is required in online mode to retrieve credentials from the directory. If this option is set to *Require smart card*, then the users single sign-on data is not accessible if the users' smartcard is not available.. **NOTE:** This preference is not available to users who have not upgraded their datastore to version 6.0.	The default value is *Allow passphrase.*
Require Smart Card is present for SSO and administration operations	*Yes*/*No*/*Default*	**NOTE:** To enable changes to this preference: ◆ The *Use smart card to encrypt SSO data* preference must be set to either *PKI Credentials* or *Key generated on smart card*. ◆ The *Lost card scenario* preference must be set to *Require Smart card*. This preference requires that a smart card must be accessible by SecureLogin each time a single sign-on operation is performed by an end user operation or administration operation. If this preference is set, SecureLogin cannot start without the smart card. As soon as the smart card is removed, SecureLogin is locked. By default, this preference is not set. If this option is set to *Yes*, Novell SecureLogin operations does not function without the smart card present. If the smart card is removed, Novell SecureLogin prompts to re-insert the card. If this option is set to *No* or *Default*, Novell SecureLogin can start without the smart card. **NOTE** ◆ If the *Lost card scenario* is set to *Allow passphrase*, the *Require smart Card is present for SSO and administration operations* preference is set to *No* and is not editable. ◆ This preference is not available to users who have not upgraded their datastore to version 6.0.	The default value is *No*.

Preference	Possible Values	Description	Default Value
Store credentials on smart card	*No*	With this release of Novell SecureLogin, this option is set to *No* and changes to this preference are disabled. You cannot change this preference to store SecureLogin credentials on smart card.	*No*
Use AES for SSO data encryption	*Yes*/*No*	This option is defined to change the data encryption mode. This option is not available prior to version 6.0 of Novell SecureLogin. If the preference is set to *Yes* or *Default*, AES encryption is used for encrypting single sign-on data. If the preference is set to *No*, Triple DES is used for encrypting single sign-on data.	The default value is *Yes*.
Use enhanced protection by default	*Yes*/*No*/*Default*	This setting is only relevant in a Novell environment; it relates to using SecretStore protection. If this option is set to *Yes* or *Default*, then a password protection is added. If this option is set to *No*, a password protection is not added. This preference is not available to users who have not upgraded their datastore to version 6.0.	The default value is *Yes*.
Use smart card to encrypt SSO data	*No*/*PKI credentials*/*Key generated on smart card*	Allows PKI credentials or a self-generated key to be created as the encryption source to encrypt the single sign-on data in the directory. If this preference is set to *No* or *Default*, all other smart card options are dimmed. If this preference is set to PKI credentials, single sign-on data is encrypted using the user's PKI credentials. Single sign-on data stored in the Directory and in the offline cache (if enabled) is encrypted using the public key from the selected certificate and the private key (stored on a PIN-protected smart card) is used for decryption. If this preference is set to *Key generated on smart card*, single sign-on data is encrypted using a randomly generated symmetric key that is stored on the user's smart card. This key is used to encrypt and decrypt single sign-on data stored in the Directory and in the offline cache (if enabled).	The default preference is *No*.

Table 2-10 *The Java Preferences Properties Table*

Preference	Possible Values	Description	Default Value
Add application prompts for Java applications	*Yes*/*No*/*Default*	This preference controls whether Novell SecureLogin detects Java application. If the preference is set to *Yes* or *Default*, Novell SecureLogin prompts to create a script when a Java application login page is loaded. Novell SecureLogin will not prompt when Java application login page is loaded. This preference is available in both the Novell SecureLogin Client Utility and all the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Allow single sign-on to Java applications	*Yes*/*No*/*Default*	This preference controls whether Novell SecureLogin allows single sign-on for Java applications. If the preference is set to *Yes* or *Default*, Novell SecureLogin prompts the user to enter credentials (if none already exist), or submits existing credentials on the Java application login page. If this option is set to *No*, Java applications are not enabled for single sign-on. This preference is available in both the Novell SecureLogin Client Utility and all the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Table 2-11 *The Web Preferences Properties Table*

Preference	Possible Values	Description	Default Value
Add application prompts for Internet Explorer	*Yes*/*No*/*Default*	This preference controls the display of the Web login detection wizard and confirmation dialog box when a Web application is detected and recognized by Internet Explorer. If you select *Yes* or *Default*, the user is initially prompted to enable the application and enter the credentials for the application (if not done previously). **NOTE:** Setting the perference to *Yes* when displayed to users depends on the settings of the Wizard mode preference. On subsequent runs of the application, the user is not prompted for credentials and single sign-on occurs seamlessly. If you select *No*, Novell SecureLogin skips enabling the application for single sign-on, the user is never be prompted to enable the application. This preference is available in both the Novell SecureLogin Client Utility and all the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Add application prompts for Mozilla Firefox	*Yes*/*No*/*Default*	This preference controls the display of Web login detection wizard and confirmation dialog box when a Web application is detected and recognized by Mozilla Firefox. **NOTE:** Setting the perference to *Yes* when displayed to users depends on the settings of the Wizard mode preference. If you select *Yes* or *Default*, the user is initially prompted to enable the application and enter the credentials for the application (if not done previously). On subsequent runs of the application, the user is not prompted for credentials and single sign-on occurs seamlessly. If you select *No*, Novell SecureLogin skips enabling the application for single sign-on on this instance. You are prompted to enable the application when you launch it the next time. This preference is available in both the Novell SecureLogin Client Utility and all the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Preference	Possible Values	Description	Default Value
Allow single sign-on to Internet Explorer	*Yes*/*No*/*Default*	This preference defines single sign-on access to Web application using Internet Explorer. If you select *Yes* or *Default* the specified credentials are saved and the application is enabled for single sign-on. If you select *No*, Novell SecureLogin does not prompt for credentials (if none exist or are incorrect) and does not submit credentials into the application. This preference is available in both the Novell SecureLogin Client Utility and all the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.
Allow single sign-on Mozilla Firefox	*Yes*/*No*/*Default*	This preference defines single sign-on access to Web application using Mozilla Firefox. If you select *Yes* or *Default* the specified credentials are saved and the application is enabled for single sign-on. If you select *No*, Novell SecureLogin does not prompt for credentials (if none exists or are incorrect) and does not submit credentials into the application. This preference is available in both the Novell SecureLogin Client Utility and all the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

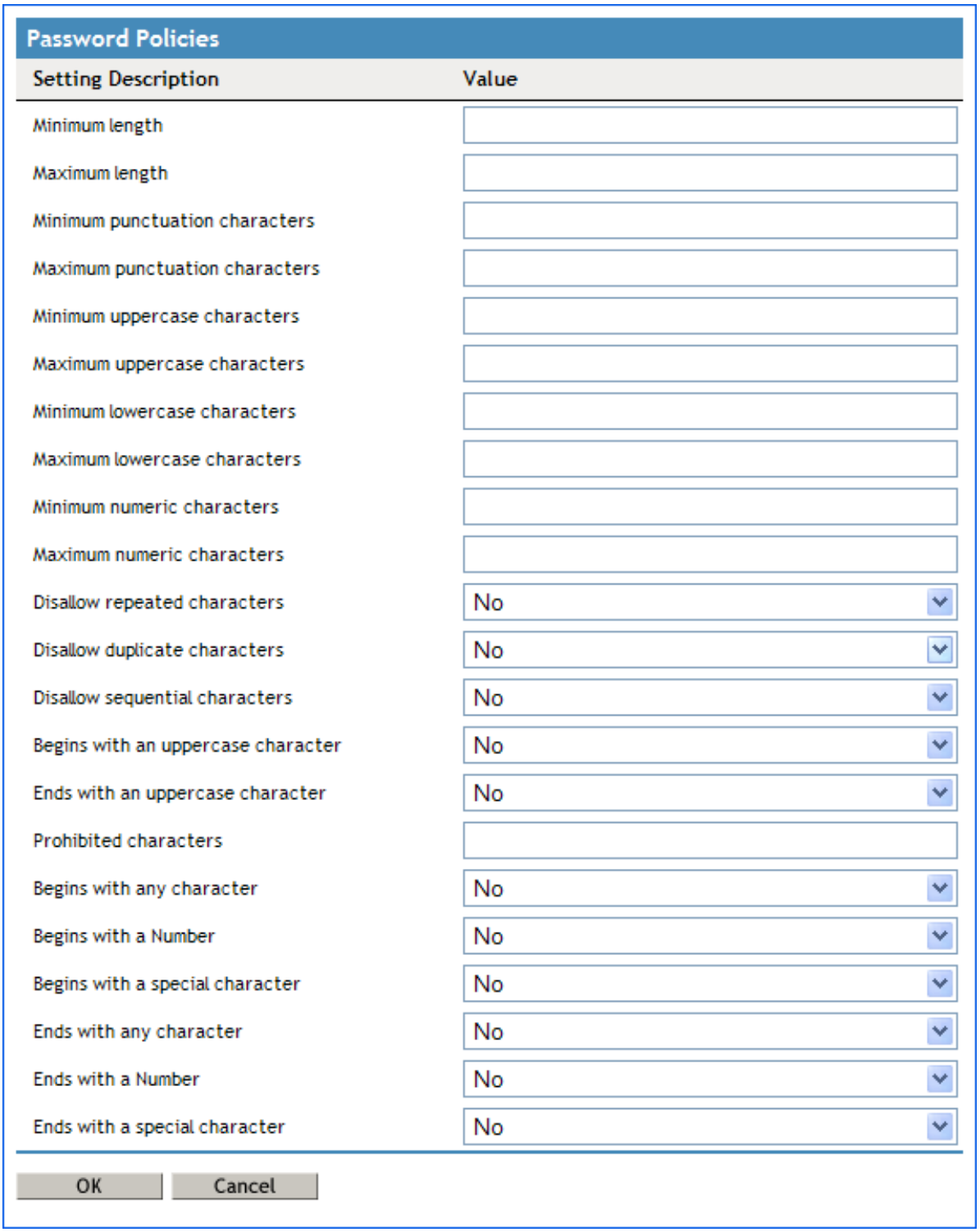
Table 2-12 *The Windows Preferences Properties Table*

Preference	Possible Values	Description	Default Value
Add application prompts for Windows applications	*Yes*/*No*/*Default*	This preference controls the display of a Windows login detection and confirmation message when a Windows application is detected and recognized. If you select *Yes* or *Default*, the user prompted to enable the application and to enter the credentials for the application (if not done previously). On subsequent runs of the application, the user is not prompted for credentials and single sign-on occurs seamlessly. If you select *No*, Novell SecureLogin skips enabling the application for single sign-on on this instance. You are prompted to enable the application when you launch it the next time. This preference is available in both the Novell SecureLogin Client Utility and all the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

Preference	Possible Values	Description	Default Value
Allow single sign-on to Windows applications	*Yes*/*No*/*Default*	This preference defines single sign-on access to Windows applications. If you select *Yes* or *Default* the specified credentials are saved and the application is enabled for single sign-on. If you select No, Novell SecureLogin will not prompt for credentials (if none exist or are incorrect) and will not submit credentials into the application. This preference is available in both the Novell SecureLogin Client Utility and all the administrative management utilities (iManager, SLManager, and MMC snap-ins).	The default value is *Yes*.

2.8 The Password Policy Properties Table

Figure 2-6 *The Password Policy Properties Table*



The Password Policies pane contains a list of all the password policies. Through this pane, a user can create a new policy or delete an existing password policy.

Organizations and applications often have rules about the content of passwords, including the required number and type of characters. The Password Policy properties table helps the users to create and enforce these password rules through a password policy, then apply this policy to one or more application logins.

Table 2-13 *The Password Policy Properties Table*

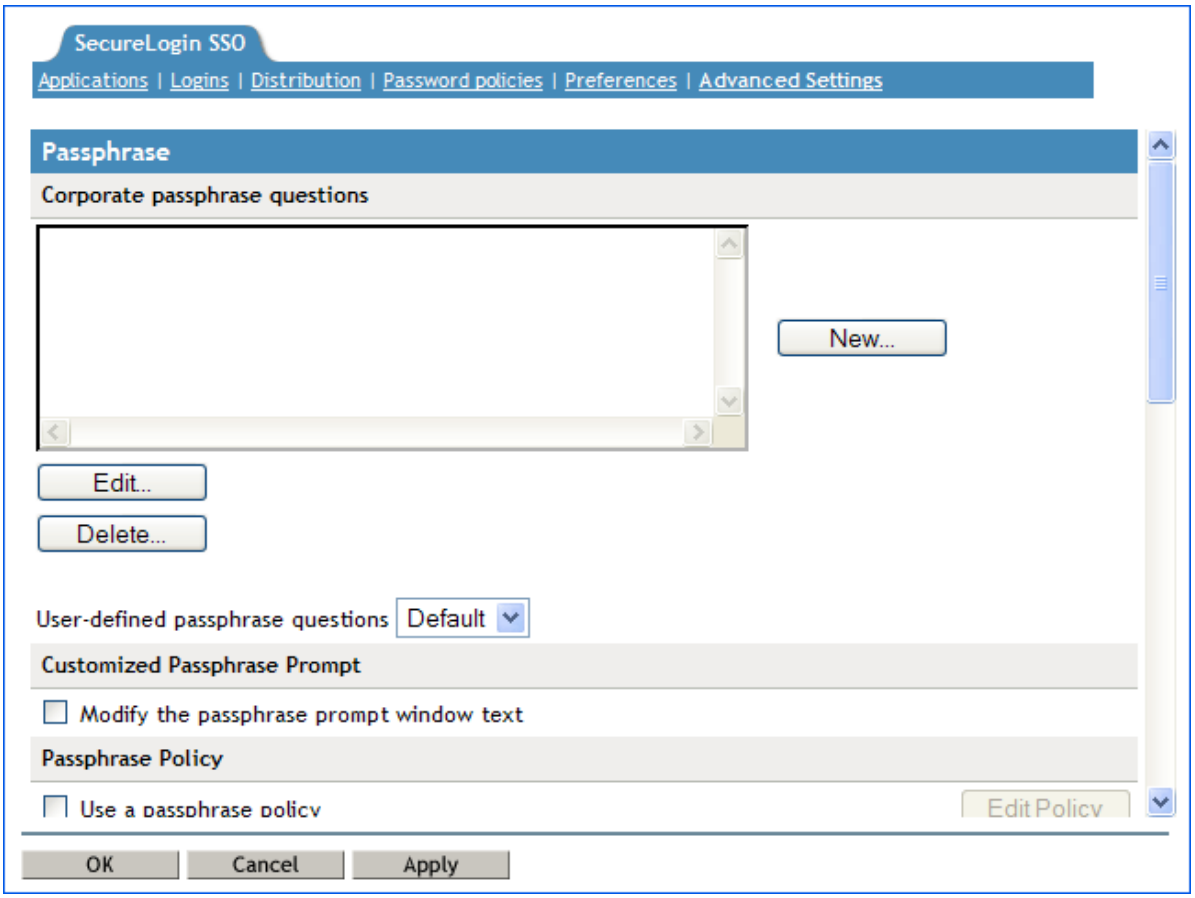
Policy	Value To Be provided	Description
Minimum length	Whole number	Defines the minimum length of the password; that is, the number of characters required for the password.
Maximum length	Whole number	Defines the maximum length of the password; that is, the maximum number of characters allowed in password.
Minimum punctuation characters	Punctuation characters	Defines the minimum number of punctuation characters allowed in a password.
Maximum punctuation characters	Punctuation characters	Defines the maximum number of punctuation characters allowed in a password.
Minimum uppercase characters	Whole number	Defines the minimum number of uppercase characters allowed in a password.
Maximum uppercase characters	Whole number	Defines the maximum number of uppercase characters allowed in a password.
Minimum lowercase characters	Whole number	Defines the minimum number of lowercase characters allowed in a password.
Maximum lowercase characters	Whole number	Defines the maximum number of lowercase characters allowed in a password.
Minimum numeric characters	Whole number	Defines the minimum number of numeric characters allowed in a password.
Maximum numeric characters	Whole number	Defines the maximum number of numeric characters allowed in a password.
Disallow repeat characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of repeated characters, or the use of the same successive characters. If this option is set to *No*, characters can be repeated. This is the default value. If this option is set to *Yes*, same alphabetic characters in a different case are considered as different characters. For example, A and a are different. If this option is set to *Yes, case insensitive*, the successive use of the same alphabetic characters in a different case is not allowed.

Policy	Value To Be provided	Description
Disallow duplicate characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of the same non-successive characters. If this option is set to *No*, duplicate characters are allowed. This is the default value. If this option is set to *Yes*, the same alphabetic characters in a different case are considered as different characters. For example, A (uppercase) and a (lowercase) are different. If this option is set to *Yes, case insensitive*, duplication of the same alphabetic characters in a different case is not allowed.
Disallow sequential characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of successive characters in an alphabetical order. If this option is set to *No*, sequential characters are allowed. This is the default value. If this option is set to *Yes*, sequential characters in a different case are considered as non-sequential. For example, a and B are non-sequential. If this option is set to *Yes, case insensitive*, sequential characters in different cases is disallowed.
Begin with an uppercase character	*No*/*Yes*	Enforces the use of an uppercase alphabetic character as the beginning character of a password. The default value is *No*. If this option is set to *Yes*, all other policies that indicate that a password must begin with a particular character or in a specific manner are disabled. **IMPORTANT:** Only one type of character can be designated as the first value of a password.
End with an uppercase character	*No*/*Yes*	Enforces the use of an uppercase letter at the end of a password. The default value is *No*. If this option is set to *Yes*, all other policies that indicate that a password must end with a particular character or in a specific manner are disabled.

Policy	Value To Be provided	Description
Prohibited characters	Keyboard characters	Defines a list of characters that cannot be used in a password. **NOTE:** There is no need of a separator in the list of prohibited characters. For example, @#$%&
Begin with any Alpha character	*No*/*Yes*	Enforces the use of an alphabetic character at the beginning of a password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the password should be.
Begin with any number	*No*/*Yes*	Enforces the use of a numeric character as the first character of the password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the password should be.
Begin with any symbol	*No*/*Yes*	Enforces the use of a symbol character as the first character of the password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the password should be.
End with any Alpha character	*No*/*Yes*	Enforces the use of an alphabetic character as the last character of the password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the password should end with.
End with any number	*No*/*Yes*	Enforces the use of a numeric character as the last character of the password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the password should end with.
End with any symbol	*No*/*Yes*	Enforces the use of a symbol character as the last character of the password. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the password should end with.

2.9 The Advanced Settings Pane

Figure 2-7 *The Advanced Settings Pane with the Passphrase Option*



The *Advanced Settings* page contains the following three tabs:

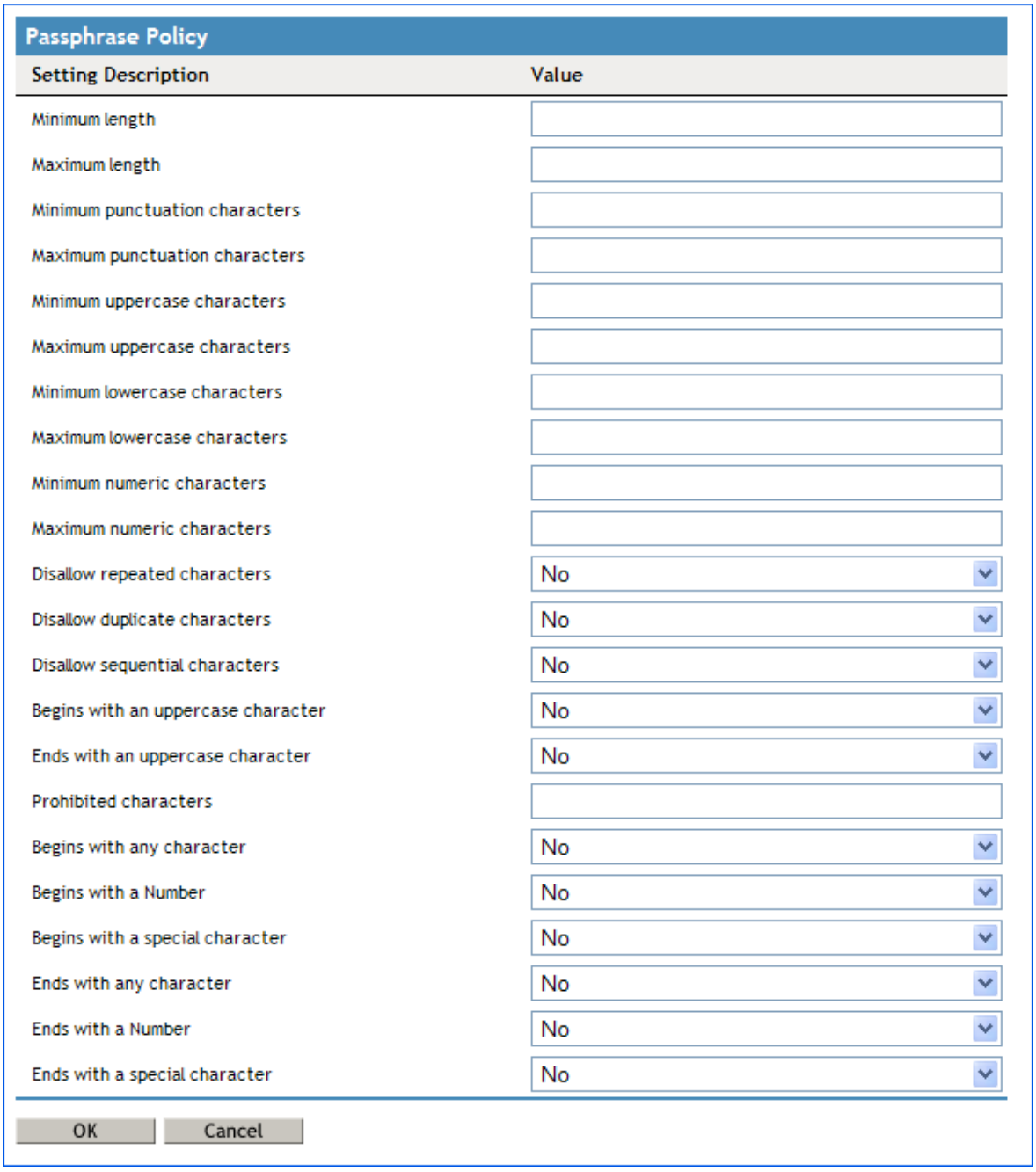
Table 2-14 *The Advanced Settings Pane*

Tab Name	Description
Passphrase	This page contains fields for: ◆ Creating, editing, and deleting corporate passphrase questions. ◆ Customizing passphrase prompts. ◆ Editing passphrase policies.
Datastore	This is used for: ◆ Selecting directory data version details (for mixed mode environments by using the earlier versions of the client software). ◆ Deleting Novell SecureLogin configuration for a datastore object.
Corporate Redirection	This is used for managing configuration from one directory object when multiple container or organizational units require the same Novell SecureLogin environment.

NOTE: The *Advanced Settings* option is not available in Novell SecureLogin Client Utility.

2.10 The Passphrase Policy Properties Table

Figure 2-8 *The Passphrase Policy Properties Table*



Organizations and applications often have rules about the content of a passphrase, including the required number and type of characters. The *Passphrase* policy properties table helps the user or the administrator to create and enforce these passphrase rules through a passphrase policy, then apply this policy to one or more application logins.

Table 2-15 *The Passphrase Policy Properties Table*

Policy	Value To Be provided	Description
Minimum length	Whole number	Defines the minimum length of the passphrase; that is, the number of characters required for the passphrase.
Maximum length	Whole number	Defines the maximum length of the passphrase; that is, the maximum number of characters allowed in passphrase.
Minimum punctuation characters	Punctuation characters	Defines the minimum number of punctuation characters allowed in a passphrase.
Maximum punctuation characters	Punctuation characters	Defines the maximum number of punctuation characters allowed in a passphrase.
Minimum uppercase characters	Whole number	Defines the minimum number of uppercase characters allowed in a passphrase.
Maximum uppercase characters	Whole number	Defines the maximum number of uppercase characters allowed in a passphrase.
Minimum lowercase characters	Whole number	Defines the minimum number of lowercase characters allowed in a passphrase.
Maximum lowercase characters	Whole number	Defines the maximum number of lowercase characters allowed in a passphrase.
Minimum numeric characters	Whole number	Defines the minimum number of numeric characters allowed in a passphrase.
Maximum numeric characters	Whole number	Defines the maximum number of numeric characters allowed in a passphrase.
Disallow repeat characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of repeated characters, or the use of the same successive characters. If this option is set to *No*, characters can be repeated. This is the default value. If this option is set to *Yes*, same alphabetic characters in a different case are considered as different characters. For example, A and a are different. If this option is set to *Yes, case insensitive*, the successive use of the same alphabetic characters in a different case is not allowed.

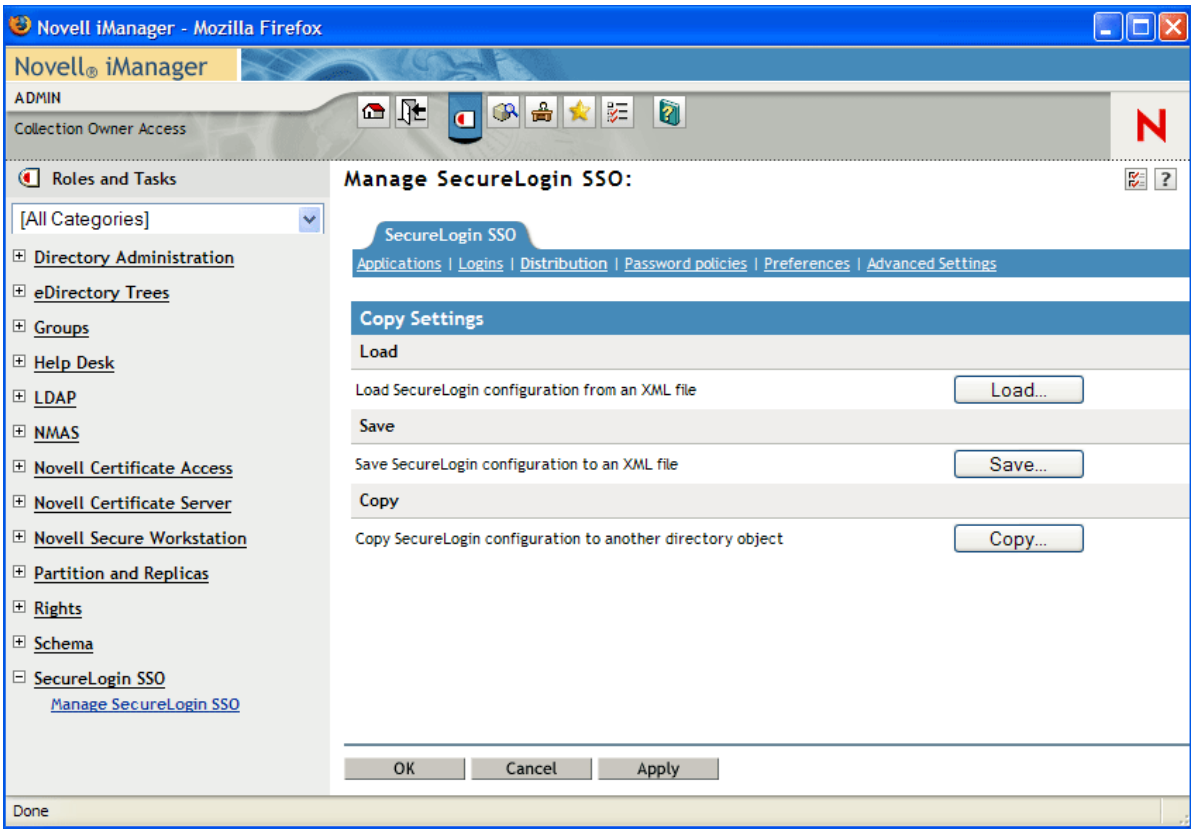
Policy	Value To Be provided	Description
Disallow duplicate characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of the same non-successive characters. If this option is set to *No*, duplicate characters are allowed. This is the default value. If this option is set to *Yes*, the same alphabetic characters in a different case are considered as different characters. For example, A (uppercase) and a (lowercase) are different. If this option is set to *Yes, case insensitive*, duplication of the same alphabetic characters in a different case is not allowed.
Disallow sequential characters	*No*/*Yes*/*Yes, case insensitive*	Disallows the use of successive characters in an alphabetical order. If this option is set to *No*, sequential characters are allowed. This is the default value. If this option is set to *Yes*, sequential characters in a different case are considered as non-sequential. For example, a and b and non-sequential. If this option is set to *Yes, case insensitive*, sequential characters in different cases is disallowed.
Begin with an uppercase character	*No*/*Yes*	Enforces the use of an uppercase alphabetic character as the beginning character of a passphrase. The default value is *No*. If this option is set to *Yes*, all other policies that indicate that a passphrase must begin with a particular character or in a specific manner are disabled. **IMPORTANT:** Only one type of character can be designated as the first value of a passphrase.
End with an uppercase character	*No*/*Yes*	Enforces the use of an uppercase letter at the end of a passphrase. The default value is *No*. If this option is set to *Yes*, all other policies that indicate that a passphrase must end with a particular character or in a specific manner are disabled.

Policy	Value To Be provided	Description
Prohibited characters	Keyboard characters	Defines a list of characters that cannot be used in a passphrase. **NOTE:** There is no need of a separator in the list of prohibited characters. For example, @#$%&
Begin with any Alpha character	*No*/*Yes*	Enforces the use of an alphabetic character at the beginning of a passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the passphrase should be.
Begin with any number	*No*/*Yes*	Enforces the use of a numeric character as the first character of the passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the passphrase should be.
Begin with any symbol	*No*/*Yes*	Enforces the use of a symbol character as the first character of the passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the first character of the passphrase should be.
End with any Alpha character	*No*/*Yes*	Enforces the use of an alphabetic character as the last character of the passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the passphrase should end with.
End with any number	*No*/*Yes*	Enforces the use of a numeric character as the last character of the passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the passphrase should end with.

Policy	Value To Be provided	Description
End with any symbol	*No*/*Yes*	Enforces the use of a symbol character as the last character of the passphrase. The default value is *No*. If this option is set to *Yes*, it automatically disables all other policies that specify what the passphrase should end with.

2.11 The Distribution Pane

Figure 2-9 *The Distributions Pane*



The *Distribution* pane provides access to:

- The Load dialog box
- The Save dialog box
- The Copy dialog box

The Load and Save dialog boxes help the administrator to import and export the SecureLogin configurations.

The Copy dialog box help the administrator to copy an object's SecureLogin configuration from one object to another.

NOTE: The *Distribution* pane is not available for Novell SecureLogin Client Utility.

3 Novell SecureLogin Components

This section discusses the following topics:

3.1 Novell SecureLogin Management Utilities

Table 3-1 *Novell SecureLogin Management Utilities*

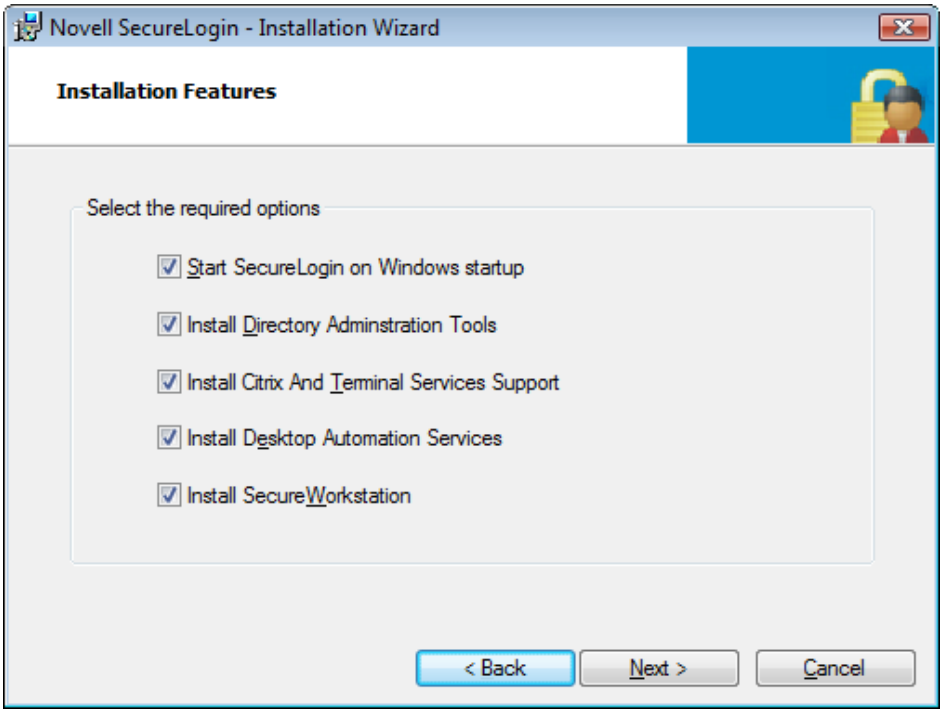
Use This Utility	To Manage These Users
Administrative Management utilities	Centrally in a directory environment at the user object, Group Policy, Container, or the Organizational Unit (OU) level. The administrative management utility includes the Novell iManager. In a corporate environment, the administrators can allow or prohibit all or part of this utility, depending on the organizational requirements.
Novell SecureLogin Client Utility	Users in the standalone mode. Users can configure the local workstation for the logged-in user. This utility has the same functionality as the Administrative Management utility, excluding some preference options, advanced settings, and secure settings distribution. Administrators can disable the users from accessing this utility in a directory environment. For more information, see Section 2.1, “Novell SecureLogin Client Utility,” on page 9
Active Directory Users and Computers snap-in	Centrally in an Active Directory environment. Using Microsoft Active Directory, Novell SecureLogin installs an administration tab in the Users and Computers Properties snap-in. This provides access to the administrative management utility functionality. In a corporate environment you can allow or prohibit full or part access to this utility depending on organizational requirements.

3.2 Active Directory Users and Computer Snap-In

In Microsoft Active Directory environment, you can manage users centrally from the Active Directory users and computer snap-in.

The snap-in and the SecureLogin Administrative Management utility is installed when you select the *Install Directory Administration Tools* during Novell SecureLogin installation.

Figure 3-1 *Installation Features*



When you select the *Install Directory Administration Tools* option during Novell SecureLogin installation:

- It installs an Administration tab in the Active Directory Microsoft Management Console (MMC). This allows you access the Administrative Management utility functionality in the Users and Computers snap-in.
- It also provides a snap-in to Active Directory Users and Computers snap-in for configuration in the Microsoft Active Directory environment.

NOTE: If you select the *Enable Microsoft Active Directory Group Policies* option during the installation, you can administer Novell SecureLogin by using the Group Policy object.

3.3 Application Definition Wizard

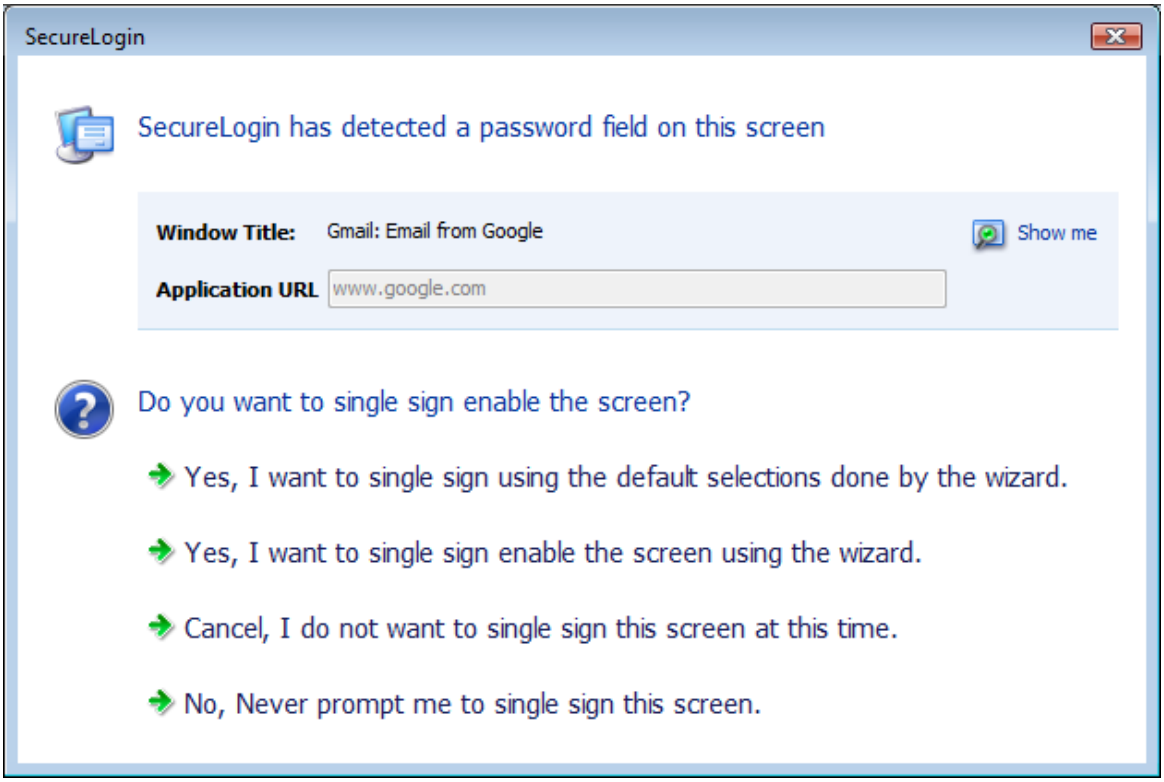
Application definitions specify how SecureLogin interacts with an application using your single sign-on (SSO) credentials. The Application Definition Wizard assists you in creating an application definitions.

IMPORTANT: You can use the Application Definition Wizard only if the administrator has given you permission. The administrator can restrict users' access to the Application Definition Wizard. Depending on the preferences set by the administrator, you might be allowed to create application definitions for new applications or you might not have access at all.

In most instances the Application Definition Wizard opens automatically when it detects a new logon screen, but you can also choose to create or modify application definitions using the wizard to automate the handling of notification screens including prompts to change your password and error messages.

For information on using to Application Definition Wizard to create application definitions and enabling applications for single sign-on, refer *Novell SecureLogin Application Definition Wizard Administration Guide*

Figure 3-2 *The Application Definition Wizard Prompts*



The Aplication Definition Wizard help you to create and change the application definition responses for the following:

- The Login Screen
- The Login Notification Screen
- The Change Password Screen
- The Change Password Notification Screen
- Application that are not recognized by the Application Definition Wizard

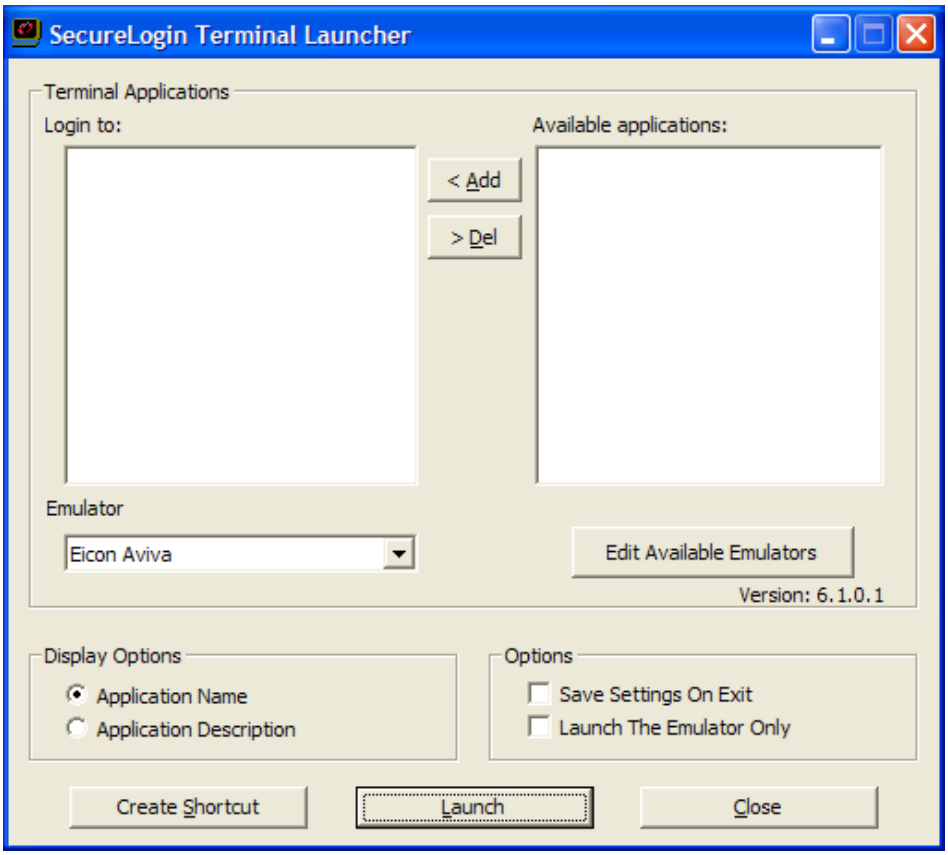
3.4 Add New Login Wizard

The Add New Login Wizard helps the users to create multiple logins for the same application or server. The Wizard contains a list of available applications from which users can choose the required login.

The users can use the `PickListAdd` and `PickListDisplay` commands to add login options for multiple users. For example, if all users in an IT group require three different log ins for a help desk application, the administrator can add a pick list to the help desk application definition, so all users inherit the list without individually adding the new log ins.

3.5 Terminal Launcher

Figure 3-3 *The Terminal Launcher*



Terminal applications require a terminal launcher to execute. After an application definition is created, the users must configure it to start the terminal launcher. With this, a shortcut is created to enable the user to run the terminal launcher and the terminal emulator from the desktop with automated single sign-on to the application or the server.

For deailed information on enabling single sign-on for terminal services, see "Enabling Terminal Emulator Applications" in the *Novell SecureLogin Administration Guide*.

4 Enabling Applications and Web Sites for Single Sign-On

Novell SecureLogin has predefined applications for single sign-on access to a wide range of commercially available applications.

Novell SecureLogin detects applications for which a predefined application exists. For example, if Novell SecureLogin detects Novell GroupWise Messenger dialog box, then it prompts the user to allow Novell SecureLogin to enable single sign-on for the application.

Predefined applications for some commonly used applications are incorporated with Novell SecureLogin, and with each new version, more applications are developed and made available to the customers.

Novell SecureLogin provides application definition wizards facilitate single sign-on to almost any new or proprietary application if a predefined application is not available. For details refer the .

Novell SecureLogin also supports enabling the single sign-on for standard terminal emulator applications.

- Users can enable single sign-on for terminal emulators by using the terminal launcher tool.
- Novell SecureLogin has additional tools such as, `Window Finder` and `LoginWatch`, which help the user to enable single sign-on for even the most difficult applications. For details, refer to the *Novell SecureLogin Application Definition Guide*.

Novell SecureLogin stores the login information requirements for applications including the following:

Credentials, but not limited to:	◆ Username ◆ UserID ◆ LoginID ◆ Password ◆ PINs ◆ Domain ◆ Database names ◆ Server IP address
Responses to dialog boxes, messages, and window events such as:	◆ Login ◆ Incorrect credentials ◆ Password expiration, including non-compliance to password rules ◆ Account locked ◆ Database unavailable

Before Novell SecureLogin can enable an application for single sign-on for a particular user, it must learn a user's application credentials so that it can encrypt and store them for future logins unless it is used in conjunction with Identity Management solutions such as Novell Identity Manager.

When a user starts an application for the first time after it is enabled for single sign-on, Novell SecureLogin prompts the user for application credentials, then encrypts and stores them in the directory against the user object. The credentials are passed automatically to the application for subsequent logins.

Automated single sign-on is achieved by using the proprietary application definitions. The application definitions are managed in directory environments through Novell SecureLogin administrative management utilities. In local and standalone deployments, the application definitions are managed in Novell SecureLogin Client Utility or distributed by using the advanced offline signed and encrypted method.

The single sign-on applications are created, modified, and deleted in the Applications pane. Users can also create application definitions with Novell SecureLogin Wizard. There a wide range of options in Novell SecureLogin to enable applications. Regardless, of the origin of the application definition when an application is enabled for single sign-on, it is added and maintained in the *Applications* properties table.

5 Operational Environment

This section contains information on the following:

5.1 Supported Environments

5.1.1 Platforms

- Microsoft Windows Vista SP1, 32-bit and 64 bit.
  - Microsoft Vista Ultimate
  - Microsoft Vista Enterprise
  - Microsoft Vista Business
- Microsoft Vista (32-bit and 64-bit)
- Microsoft Windows Server 2003 (32-bit and 64-bit)
- Microsoft Windows Server 2003 R2 (32-bit and 64-bit)
- Microsoft Windows Server 2008 (32-bit and 64-bit)
- Microsoft Windows Server 2008 R2 (32-bit and 64-bit)
- Microsoft Windows XP Professional SP2 and SP3 (32-bit only)
- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows 8 (32-bit and 64-bit)
- Sun ONE Directory Server 5.2
- Citrix Clients (32-bit and 64-bit)

NOTE: Microsoft Windows Server 2003 (32-bit) is supported in the Active Directory mode only; and, it is not supported in the eDirectory mode.

Windows Patch Pre-requisite for Flash SSO

- Update for Windows XP (KB971513)

  (http://www.microsoft.com/downloads/en/details.aspx?FamilyID=CD55456D-9703-42A0-B982-8A8A89CA0AA3)
- Update for Windows Server 2003 (KB971513)

  (http://www.microsoft.com/downloads/en/details.aspx?FamilyId=05101d13-1bbf-407e-80bd-4a538d96590e&displaylang=en)
- Update for Windows Server 2008 (KB971513)

  (http://www.microsoft.com/downloads/en/details.aspx?FamilyID=468E4F78-D411-4932-8719-76A0B2EB1443)

5.1.2 Clients

- Citrix Win32 ICA Client version 11.0
- Microsoft Terminal Services Clients, RDP version 6.0
- Novell Client for Windows XP and 2003, version 4.91 SP4 and SP5
- Novell Client for Windows Vista SP1

If your environment is not included in this list, contact Novell Support for assistance.

5.1.3 Support for .NET Framework

This version of Novell SecureLogin supports .NET Framework 3.5 SP1 or above. Novell SecureLogin can use only an already available .NET Framework.

5.1.4 Flash

- Adobe Flash Player 10.1 or later.

5.2 Windows

The following is a list of predefined applications for Windows applications:

- ActiveSync
- Cisco VPN
- Citrix Program Neighborhood
- Citrix Program Neighborhood - Farm Login Failure
- Citrix Program Neighborhood - Server
- Citrix Program Neighborhood - Agent
- Citrix Program Neighborhood - Agent v10.x
- GroupWise Windows Application v5.5, v6.0, v7.0, and v8.0
- Lotus Notes R8
- MEDITECH *x* and 4.*x*

NOTE: The support for MEDITECH 3.*x* and 4.*x* is dependant on the presence of the MEDITECH `mrwscript.dll` file. The `.dll` file is provided by MEDITECH and must be installed during the installation of the MEDITECH application workstation.

- Microsoft Internet Explorer 6, 7, and 8
- Microsoft Networking Client
- Microsoft Outlook
- Microsoft Outlook Express
- Microsoft SQL
- Microsoft Windows Live ID
- MSN Messenger 4.5 and 4.7
- Novell Groupwise Messenger 2.0
- Novell Groupwise Notify Client
- Novell Groupwise 7.0 Web Login
- Novell iManager Web Login
- Quick Finder
- SAP - `SAPlogon.exe`
- SAP R/3 Login
- Trillian
- VNC 3.0 and 4.0
- Windows Live Messenger 5.0, 6.0, 7.5, 8.1, and 2009
- Windows Remote Desktop 6
- Yahoo! Messenger 8.1
- Yahoo! Messenger 8.1 Alternate

If Novell SecureLogin does not prompt to enable single sign-on for applications, use the Application Definition Wizard to build an application.

5.3 Flash SSO Script Support

5.3.1 Prerequisites

- Adobe Flash Player 10.1 or later.
- Windows patch prerequisite for Flash SSO. This includes the Microsoft Active Acessibility libraries for Windows XP, Windows Server 2003, and Windows Sever 2008.
  - Download the update for Windows XP (KB971513) from the Microsoft Download Center (http://www.microsoft.com/downloads/en/details.aspx?FamilyID=CD55456D-9703-42A0-B982-8A8A89CA0AA3).

- Download the update for Windows Server 2003 (KB971513) from the Microsoft Download Center (http://www.microsoft.com/downloads/en/details.aspx?FamilyId=05101d13-1bbf-407e-80bd-4a538d96590e&displaylang=en).
- Download the update for Windows Server 2008 (KB971513) from the Microsoft Download Center (http://www.microsoft.com/downloads/en/details.aspx?FamilyID=468E4F78-D411-4932-8719-76A0B2EB1443).

5.3.2 Registry Configuration

- "Disabling Flash SSO" on page 60
- "Enabling Flash SSO Debug Log" on page 60

Disabling Flash SSO

1. Click *Start* > *Run* > type `regedit` in the Run dialog box to launch the Registry Editor.
2. Browse to the `HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\Securelogin` key.
3. Create a DWORD and name it *DisableFlashSSO*.
4. To disable Flash SSO, set *DisableFlashSSO* to 1.

NOTE: To enable Flash SSO, set *DisableFlashSSO* to 0 (default) .

Enabling Flash SSO Debug Log

1. Click *Start* > *Run* > type `regedit` in the Run dialog box to launch the Registry Editor.
2. Browse to the `HKEY_LOCAL_MACHINE\SOFTWARE\Protocom\SecureLogin\Logging` key.
3. Create a DWORD and name it *winsso*.
4. To enable the debug log, set *winsso* to 0.

5.4 Terminal Servers

Novell SecureLogin supports the following terminal servers:

- Citrix Presentation Server 4.5 (32-bit and 64-bit)
- Citrix XenApp 5.0 (32-bit and 64-bit)
- Microsoft Windows Terminal Server 2003 (32-bit and 64-bit)
- Microsoft Windows Terminal Server 2008 (32-bit and 64-bit)

5.4.1 Support on Microsoft Windows Vista

Citrix and Terminal Services support is always installed when Novell SecureLogin is deployed to a Vista client or workstation. The *Install Citrix and Terminal Services support* option is not displayed.

5.5 Terminal Emulators

Novell SecureLogin provides single sign-on support for the applications running on any back end system for example, UNIX, RACF, CICS, ACF2 using the following emulators:

- AbsoluteTelnet
- Attachmate Extra
- Attachmate Extra 2000
- Attachmate KEA!
- Attachmate Personal Client
- Chameleon HostLink
- CRT
- Eicon Aviva
- GLink
- HBO Star Navigator
- IBM Personal Communications
- IDXTerm Healthcare
- Info Connect
- Microsoft Telnet 2000
- Microsoft Telnet NT
- Microsoft Telnet Win 9*x*
- Mocha W32 Telnet
- NetTerm 4.2
- NS/Elite
- Passport TN 3270E
- PowerTerm
- QVT
- QWS3270 Plus
- SDI TN3270
- TeraTermPro
- TinyTERM
- ViewNow
- Wall Data Rumba
- Wall Data Rumba 2000
- Wall Data Rumba Web To Host
- WinComm
- Window Telnet VT
- WRQ Reflection

5.6 Web or Internet

Novell SecureLogin includes single sign-on support for Web applications accessed by using the following browsers:

- Internet Explorer 6.0, 7.0, and 8.0
- Mozilla Firefox 2.0, 3.0, and 3.5

Novell SecureLogin provides predefined applications for a number of Web applications with embedded login fields including:

- Citrix Web Portal
- CNN Member Services
- eBay
- Fidelity.com Web Login
- Hotmail
- Onebox.com
- Qantas Frequent Flyer
- Yahoo! Mail
- Monster.com

Novell SecureLogin prompts you if a predefined application is available. You can also use the Application Definition Wizard to build an application definition for the application.

Glossary

administrative management utilities. The utility available in Novell SecureLogin to manage the users in a directory environment. It provides additional functionality that is not available in Novell SecureLogin Client Utility.

application programming Interface. Enables programmatic communication with the application.

application definition. Novell SecureLogin configuration data that enables the single sign-on for a specific application's login and other events.

cache. The cache encrypts the local copy of Novell SecureLogin data so that a user can continue to use Novell SecureLogin even if the directory is unavailable. In a standalone mode (non-directory) mode, the cache contains all Novell SecureLogin single sign-on data for a user.

User data includes credentials, preferences, password policies, and application definitions. By default, Novell SecureLogin cache is created on the local hard drive. In a corporate implementation, this data is also stored in the directory. The data in the directory and the workstation cache are regularly synchronized to ensure that the user data is current.

container. The Microsoft Active Directory object used to contain other directory objects.

corporate configuration. Allows the administrators in a directory environment to configure where Novell SecureLogin setting on objects are inherited from.

credentials. Usernames, passwords, and other data that uniquely identifies and authenticates a user to an application.

Directory Services. Structured repository that identifies all aspects of a network. It is made up of users, software, hardware, and any rights or policies assigned.

distinguished name. The full name of a directory object, including the domain name and organizational units to which the user belongs.

domain. A security boundary that groups users or devices. Domain objects are defined by schema, configuration, and security policies of the network.

Group policy. The Group policy enables the centralized configuration and management of selected objects. User or computers are selected by the administrators to be included in the group policy group for collective administration.

High Level Language Application Programming Interface (HLLAPI). The API that enables a terminal emulator screen to read and be interpreted by an application and enables the keyboard input to be processed by the emulator.

Lightweight Directory Access Protocol (LDAP). The protocol used for updating and searching directories running over TCP/IP.

login. The set of credentials (such as username and password) stored in Novell SecureLogin.

management utility. Novell SecureLogin's management utility. It generically refers to the administrative management utilities and Novell SecureLogin Client Utility.

object. In a directory environment, a set of attributes that identifies a user, hardware, or an application.

organizational unit (ou). In a directory environment, a domain subgroup that has administrative control of all the associated objects.

passphrase. A combination of a question and answer used to protect the user credentials from unauthorized use.

password policy. One or more password rule grouped under a unique name.

password rule. A password parameter configured in the Password Policies properties table. Password rules are grouped under a Password policy.

Novell SecureLogin Client Utility. Provides user administration tools to the user from his or her desktop.

predefined application. Automates single sign-on for many commercially available applications.

Schema. A database for the classes (tables). It defines the objects and the attributes (columns) and stores the object data.

Novell SecureLogin. The application that allows users to access a wide range of applications, Web sites, and mainframe sessions. With this, users need not log in to the application separately.

SecureLogin Attribute Provisioning (SLAP). The tool that enables Novell SecureLogin to leverage user data from an organization's provisioning system.

Single Sign-On-Enabled. When an application is enabled for single sign-on for a user, the user need not specify his or her credentials to log in to the application. When the user launches an application, Novell SecureLogin transparently manages the login process.